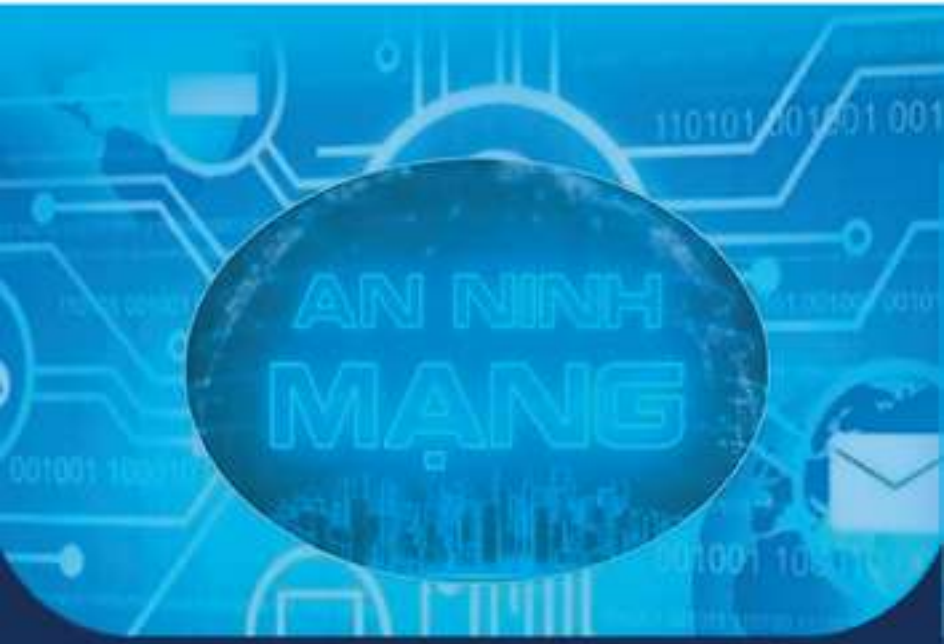
Tủ sách

HỘI ĐỒNG CHỈ ĐẠO XUẤT BẢN
SÁCH XÃ, PHƯỜNG, THỊ TRẤN

TÌM HIỂU VỀ

LUẬT AN NINH MẠNG
(HIỆN HÀNH)



NHÀ XUẤT BẢN CHÍNH TRỊ QUỐC GIA SỰ THẬT

HỎI - ĐÁP

CHÍNH SÁCH, PHÁP LUẬT VỀ PHÒNG, CHỐNG MUA BÁN NGƯỜI

HỘI ĐỒNG CHỈ ĐẠO XUẤT BẢN

Chủ tịch Hội đồng

Phó Trưởng Ban Tuyên giáo Trung ương

LÊ MẠNH HÙNG

Phó Chủ tịch Hội đồng

Q. Giám đốc - Tổng Biên tập

Nhà xuất bản Chính trị quốc gia Sự thật

PHẠM CHÍ THÀNH

Thành viên

VŨ TRỌNG LÂM

NGUYỄN ĐỨC TÀI

TRẦN THANH LÂM

NGUYỄN HOÀI ANH

HÀ NGỌC HẢI
LÊ VĂN THÀNH
NGUYỄN THỊ THU HƯƠNG
NGUYỄN NGỌC KHÁNH LINH

TÌM HIỂU VỀ
LUẬT AN NINH MẠNG
(HIỆN HÀNH)

NHÀ XUẤT BẢN CHÍNH TRỊ QUỐC GIA SỰ THẬT
Hà Nội - 2019

LỜI NHÀ XUẤT BẢN

Cuộc cách mạng công nghiệp lần thứ tư đang diễn ra mạnh mẽ, việc ứng dụng các công nghệ của cách mạng công nghiệp lần thứ tư, như: trí tuệ nhân tạo (AI), dữ liệu lớn (big data), internet vạn vật (IoT),... đã làm không gian mạng thay đổi sâu sắc, dự báo sẽ mang lại những lợi ích chưa từng có nhưng cũng làm xuất hiện những nguy cơ tiềm ẩn vô cùng lớn.

Ở Việt Nam, việc ứng dụng và phát triển mạnh mẽ công nghệ thông tin trong các lĩnh vực của đời sống đã góp phần đẩy nhanh quá trình công nghiệp hóa, hiện đại hóa, phát triển kinh tế - xã hội của đất nước. Tuy nhiên, không gian mạng ở nước ta cũng xuất hiện nhiều nguy cơ, thách thức lớn tác động trực tiếp đến an ninh quốc gia, trật tự, an toàn xã hội. Do vậy, bên cạnh việc cần khai thác tối đa ưu thế của cách mạng công nghệ, của không gian mạng là yêu cầu cấp thiết phải xây dựng và ban hành luật về an ninh mạng để quản lý, phòng ngừa, đấu tranh, xử lý các hành vi sử dụng không gian mạng xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của tổ chức, cá nhân.

Ngày 12/6/2018, tại kỳ họp thứ 5, Quốc hội khóa XIV đã thông qua Luật An ninh mạng. Luật gồm 7 chương, 43 điều quy định về hoạt động bảo vệ an ninh mạng và bảo đảm trật tự, an toàn xã hội trên không gian mạng;

trách nhiệm của cơ quan, tổ chức, cá nhân có liên quan. Đây là cơ sở pháp lý quan trọng để phòng ngừa, đấu tranh, xử lý các hoạt động vi phạm pháp luật trên không gian mạng, bảo vệ quyền và lợi ích hợp pháp của tổ chức, cá nhân; tạo hành lang pháp lý để nâng cao năng lực bảo vệ hệ thống thông tin quan trọng về an ninh quốc gia, góp phần bảo vệ chủ quyền, an ninh, trật tự và xây dựng không gian mạng an toàn, lành mạnh.

Để tạo điều kiện cho việc tìm hiểu, áp dụng, triển khai thi hành Luật An ninh mạng, giúp cán bộ, đảng viên và Nhân dân tại các cơ sở xã, phường, thị trấn hiểu rõ những nội dung cơ bản của Luật này, Nhà xuất bản Chính trị quốc gia Sự thật xuất bản cuốn sách ***Tìm hiểu về Luật An ninh mạng (hiện hành)*** do tập thể tác giả Hà Ngọc Hải, Lê Văn Thành, Nguyễn Thị Thu Hương, Nguyễn Ngọc Khánh Linh biên soạn. Cuốn sách gồm 05 phần:

Phần I - Tổng quan về Luật An ninh mạng năm 2018.

Phần II - Những nội dung cơ bản của Luật An ninh mạng năm 2018.

Phần III - Trách nhiệm của các cá nhân, tổ chức trong bảo vệ an ninh mạng.

Phần IV - Một số nội dung Nhân dân, doanh nghiệp quan tâm trong Luật An ninh mạng năm 2018.

Phần V - Một số vấn đề đặt ra khi triển khai thi hành Luật An ninh mạng năm 2018 trong cơ quan, tổ chức.

Xin giới thiệu cuốn sách với bạn đọc.

Tháng 8 năm 2019

NHÀ XUẤT BẢN CHÍNH TRỊ QUỐC GIA SỰ THẬT

Phần I

TỔNG QUAN VỀ LUẬT AN NINH MẠNG NĂM 2018

I. SỰ CẦN THIẾT BAN HÀNH LUẬT

Thế giới đang được chứng kiến cuộc cách mạng công nghiệp lần thứ tư với sự phát triển bùng nổ của khoa học - công nghệ. Trong bối cảnh đó, không gian mạng đã xâm nhập sâu rộng, trở thành động lực trong phát triển kinh tế - xã hội của mọi quốc gia; làm thay đổi cơ bản cách tiếp cận tri thức của con người trên tất cả các lĩnh vực. Với đặc tính của mình, những lợi ích mà không gian mạng đem lại là vô cùng lớn nhưng đi kèm với nó là những thách thức, nguy cơ tác động trực tiếp đến chủ quyền, an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của các tổ chức, cá nhân.

Bảo vệ quyền, lợi ích và an ninh quốc gia trên không gian mạng và ứng phó với những nguy cơ đến từ không gian mạng đã và đang trở thành vấn đề toàn cầu, được xác định là nhiệm vụ chiến lược ở nhiều quốc gia trên thế giới. Trên cơ sở đó,

các nước đã ban hành các văn bản quy phạm pháp luật để điều chỉnh hành vi của con người, mối quan hệ xã hội trên không gian mạng, góp phần nâng cao năng lực bảo vệ an ninh mạng và phòng ngừa, đấu tranh, xử lý các hành vi vi phạm pháp luật trên không gian mạng. Theo báo cáo của Liên hợp quốc đến năm 2018 đã có 138 quốc gia (trong đó có 95 nước đang phát triển) ban hành ít nhất một đạo luật về an ninh mạng[1]; đặc biệt, những nước có trình độ phát triển kinh tế, khoa học - công nghệ hàng đầu thế giới như Hoa Kỳ, Nga, Trung Quốc, Nhật Bản, Đức... đã đặt vấn đề nghiên cứu, xây dựng, ban hành các đạo luật về an ninh mạng từ rất sớm.

Việt Nam là một trong các quốc gia có tốc độ phát triển công nghệ thông tin nói chung, internet nói riêng nhanh nhất thế giới, không gian mạng đã góp phần tích cực phục vụ phát triển kinh tế - xã hội, nâng cao chất lượng y tế, giáo dục, phát huy sức sáng tạo và quyền làm chủ của Nhân dân, góp phần thúc đẩy quá trình công nghiệp hóa, hiện đại hóa đất nước. Tuy nhiên, theo số liệu của các tổ chức hàng đầu thế giới về an ninh mạng thì những năm qua Việt Nam luôn nằm trong tốp những quốc gia có chỉ số an ninh mạng thấp nhất

---

1. Phạm Nguyễn: *Bảo vệ an ninh mạng là chính vì lợi ích quốc gia, vì lợi ích mọi người,* https://nhandan.com.vn, truy cập ngày 19/6/2018.

thế giới, bị tấn công mạng nhiều nhất. Không gian mạng ở nước ta cũng xuất hiện nhiều nguy cơ, thách thức lớn tác động trực tiếp đến an ninh quốc gia, trật tự, an toàn xã hội, cụ thể như sau:

Thứ nhất, tiềm lực quốc gia về an ninh mạng của nước ta chưa đủ mạnh để đối phó với các mối đe dọa trên không gian mạng. Mặc dù chúng ta đã có nhiều chính sách nhằm thúc đẩy cho việc phát triển nền kinh tế số nhưng hệ thống pháp luật về an ninh mạng ở nước ta còn chưa hoàn thiện và chưa thực sự đi vào cuộc sống; cơ sở hạ tầng kỹ thuật của nước ta còn yếu, thiếu đồng bộ, phụ thuộc vào thiết bị công nghệ có nguồn gốc từ nước ngoài; nguồn nhân lực chất lượng cao chưa đáp ứng về số lượng cũng như đáp ứng yêu cầu của thực tiễn đặt ra; lực lượng chuyên trách về an ninh mạng còn hạn chế, chỉ tập trung ở cấp trung ương; hợp tác quốc tế về an ninh mạng mặc dù đã có những bước tiến tích cực nhưng chưa thực sự đi vào chiều sâu.

Thứ hai, không gian mạng đang bị các thế lực thù địch, phản động và bọn tội phạm sử dụng để tiến hành các hoạt động xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, đặc biệt là hoạt động tuyên truyền chống phá chế độ, kích động biểu tình, bạo loạn, thực hiện "cách mạng màu", "cách mạng đường phố", "phá hoại chính trị nội bộ" nhằm thay đổi thể chế chính trị tại Việt Nam. Tình trạng tin giả, tin xấu, độc, sai sự thật được đăng tải tràn

lan trên không gian mạng nhưng chưa có biện pháp quản lý hữu hiệu, làm ảnh hưởng tới chủ quyền, lợi ích, an ninh, trật tự, tổn hại đến quyền và lợi ích hợp pháp của tổ chức, cá nhân.

Thứ ba, tại Việt Nam xuất hiện nhiều cuộc tấn công mạng với quy mô lớn, cường độ cao, với tính chất, mức độ ngày càng nguy hiểm, đe dọa trực tiếp đến an ninh quốc gia và trật tự, an toàn xã hội. Nhiều cuộc tấn công mạng có chủ đích (APT) được tiến hành nhằm vào các hệ thống thông tin trọng yếu của Đảng, Nhà nước, các doanh nghiệp, tập đoàn kinh tế để phá hoại, kiểm soát, khống chế hệ thống mạng và chiếm đoạt thông tin, tài liệu bí mật nhà nước, tài liệu nội bộ, gây ra những hậu quả nghiêm trọng về an ninh, chính trị, kinh tế. Trong khi đó, danh mục các hệ thống thông tin quan trọng về an ninh quốc gia đang trong quá trình xây dựng nên khi xảy ra các sự cố ảnh hưởng tới chủ quyền, lợi ích, an ninh quốc gia, trật tự, an toàn xã hội, việc triển khai hoạt động ứng phó, xử lý, khắc phục của các cơ quan chức năng còn nhiều khó khăn, bất cập.

Thứ tư, tình hình lộ, lọt bí mật nhà nước qua không gian mạng rất đáng lo ngại, xảy ra ở nhiều bộ, ngành, địa phương, doanh nghiệp nhà nước với nhiều biểu hiện và hình thức khác nhau. Nguyên nhân chủ yếu dẫn tới tình trạng này là do nhận thức của các cơ quan, doanh nghiệp và cá nhân về bảo vệ bí mật nhà nước trên không gian mạng còn

hạn chế; ý thức trách nhiệm của nhiều cán bộ, nhân viên trong bảo mật thông tin trên không gian mạng chưa cao, chế tài xử phạt chưa thực sự nghiêm khắc.

Thứ năm, hoạt động tội phạm mạng và những hành vi vi phạm pháp luật trên không gian mạng ngày càng gia tăng về số vụ, thủ đoạn tinh vi, gây thiệt hại nghiêm trọng trên các lĩnh vực của đời sống xã hội. Đặc biệt là hoạt động lừa đảo chiếm đoạt tài sản, tổ chức đánh bạc qua mạng ngày càng gia tăng. Hiện nay, nước ta có khoảng trên 500 trò chơi trực tuyến được phê duyệt nội dung với 33 triệu người chơi, doanh thu đạt hơn 380 triệu USD/năm; trong khi đó, có khoảng 40 trò chơi trực tuyến trái phép với quy mô lớn, rất lớn mô phỏng đánh bạc có dấu hiệu vi phạm pháp luật với hệ thống đại lý ở các địa phương trên cả nước[1].

Từ những thực trạng, nguy cơ trên và để bảo đảm Hiến pháp năm 2013 về quyền con người, quyền cơ bản của công dân và cùng với vấn đề bảo vệ Tổ quốc trong tình hình hiện nay đã đặt ra yêu cầu cấp thiết để Việt Nam xây dựng, ban hành một đạo luật về an ninh mạng. Đây là cơ sở pháp lý quan trọng để phòng ngừa, đấu tranh, xử lý các hoạt động vi phạm pháp luật trên không gian

---

1. Nguồn: Theo số liệu của Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Bộ Công an *(TG).*

mạng, bảo vệ quyền và lợi ích hợp pháp của tổ chức, cá nhân; tạo hành lang pháp lý để nâng cao năng lực bảo vệ hệ thống thông tin quan trọng về an ninh quốc gia, góp phần bảo đảm chủ quyền, an ninh, trật tự và xây dựng không gian mạng an toàn, lành mạnh.

II. MỤC TIÊU, QUAN ĐIỂM KHI XÂY DỰNG LUẬT

1. Về mục tiêu

a) Hoàn thiện cơ sở pháp lý ổn định về an ninh mạng theo hướng áp dụng các quy định pháp luật đồng bộ, khả thi trong thực tiễn thi hành.

b) Phát huy các nguồn lực của đất nước để bảo đảm an ninh mạng, phát triển lĩnh vực an ninh mạng đáp ứng yêu cầu phát triển kinh tế - xã hội, quốc phòng, an ninh, góp phần nâng cao chất lượng cuộc sống của Nhân dân và bảo đảm quốc phòng, an ninh.

c) Bảo vệ chủ quyền, lợi ích, an ninh quốc gia, quyền và lợi ích hợp pháp của tổ chức, cá nhân tham gia hoạt động trên không gian mạng, xây dựng môi trường không gian mạng lành mạnh.

d) Triển khai công tác an ninh mạng trên phạm vi toàn quốc, đẩy mạnh công tác giám sát, dự báo, ứng phó và diễn tập ứng phó sự cố an ninh mạng, bảo vệ hệ thống thông tin quan trọng về

an ninh quốc gia; đảm bảo hiệu quả công tác quản lý nhà nước trong lĩnh vực này.

đ) Nâng cao năng lực tự chủ về an ninh mạng, hoàn thiện chính sách nghiên cứu, phát triển chiến lược, chia sẻ thông tin về an ninh mạng.

e) Mở rộng hợp tác quốc tế về an ninh mạng trên cơ sở tôn trọng độc lập, chủ quyền, bình đẳng, cùng có lợi, phù hợp với pháp luật Việt Nam và điều ước quốc tế mà Việt Nam tham gia ký kết.

2. Về quan điểm chỉ đạo

Luật An ninh mạng được xây dựng trên cơ sở các quan điểm chỉ đạo sau:

Một là, thể chế hóa đầy đủ, kịp thời các chủ trương, đường lối, chính sách của Đảng, Nhà nước về an ninh mạng. Xác định bảo đảm an ninh mạng là một bộ phận cấu thành đặc biệt quan trọng của sự nghiệp bảo vệ Tổ quốc Việt Nam xã hội chủ nghĩa; là nhiệm vụ vừa cấp bách, vừa lâu dài của cả hệ thống chính trị, giao Bộ Công an chủ trì, đặt dưới sự lãnh đạo xuyên suốt của Đảng và sự quản lý thống nhất của Nhà nước.

Hai là, bảo đảm phù hợp với quy định của Hiến pháp năm 2013; cụ thể hóa các quy định của Hiến pháp, nhất là quy định về bảo vệ Tổ quốc và quy định về quyền con người, quyền và nghĩa vụ cơ bản của công dân.

Ba là, bảo đảm tính đồng bộ, thống nhất của hệ thống pháp luật, xác định hợp lý mối quan hệ giữa Luật này và các luật liên quan.

Bốn là, kế thừa các quy định hiện hành còn phù hợp, sửa đổi, bổ sung các quy định đã bộc lộ những hạn chế.

Năm là, tham khảo có chọn lọc kinh nghiệm của các nước trong khu vực và trên thế giới để vận dụng linh hoạt vào điều kiện thực tiễn của Việt Nam; bảo đảm sự phù hợp với các quy định, cam kết quốc tế mà Việt Nam tham gia ký kết hoặc là thành viên.

III. QUÁ TRÌNH XÂY DỰNG LUẬT

Trước yêu cầu cấp bách của tình hình an ninh mạng trong bảo vệ an ninh quốc gia, bảo đảm trật tự, an toàn xã hội; khắc phục những hạn chế, yếu kém cơ bản trong công tác bảo vệ an ninh mạng; thể chế hóa đầy đủ, kịp thời các chủ trương, đường lối của Đảng về an ninh mạng; bảo đảm sự phù hợp với quy định của Hiến pháp năm 2013 về quyền con người, quyền cơ bản của công dân và bảo vệ Tổ quốc, tháng 01/2016, Bộ Công an đã đề xuất xây dựng Luật An ninh mạng.

Tháng 7 năm 2016, Quốc hội ban hành Nghị quyết số 22/2016/QH14 của Quốc hội khóa XIV về điều chỉnh chương trình xây dựng luật, pháp lệnh năm 2016 và năm 2017. Thực hiện Nghị quyết

số 22/2016/QH14 của Quốc hội, ngày 23/9/2016, Thủ tướng Chính phủ đã ban hành Quyết định số 1840/2016/QĐ-TTg về phân công cơ quan chủ trì soạn thảo và thời hạn trình các dự án luật, pháp lệnh, nghị quyết được bổ sung vào Chương trình xây dựng luật, pháp lệnh năm 2016 và Chương trình xây dựng luật, pháp lệnh năm 2017. Theo đó, dự án Luật An ninh mạng được giao cho Bộ Công an chủ trì, phối hợp với các bộ, ngành có liên quan xây dựng và dự kiến trình Quốc hội cho ý kiến tại kỳ họp thứ 4 và thông qua tại kỳ họp thứ 5.

Luật An ninh mạng được xây dựng bảo đảm trình tự, thủ tục theo quy định của Luật Ban hành văn bản quy phạm pháp luật, cụ thể:

(1) Rà soát, tổng kết, đánh giá thực hiện các văn bản quy phạm pháp luật về an ninh mạng và các quy định khác liên quan đến an ninh mạng.

(2) Tổ chức nghiên cứu khoa học, nghiên cứu chuyên đề về an ninh mạng; thành lập các nhóm nghiên cứu và hoàn thành các báo cáo chuyên đề phục vụ việc xây dựng dự thảo Luật An ninh mạng.

(3) Tham khảo kinh nghiệm của một số quốc gia trong khu vực và trên thế giới về an ninh mạng, đặc biệt là Hoa Kỳ, Đức, Anh, Ôxtrâylia, Nhật Bản, Trung Quốc...

(4) Xây dựng dự án Luật An ninh mạng đúng quy trình theo pháp luật về thẩm quyền ban hành văn bản quy phạm pháp luật.

Ban soạn thảo xây dựng Luật An ninh mạng bao gồm thành viên của nhiều bộ, ngành liên

quan đã họp nhiều lần để thảo luận và quyết định những nội dung quan trọng của Luật.

Cơ quan chủ trì xây dựng dự án Luật An ninh mạng đã tổ chức lấy ý kiến đóng góp trực tiếp thông qua các tọa đàm, hội thảo như Hội thảo "Bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia" với sự tham gia của hơn 300 đại biểu đến từ các cơ quan quản lý nhà nước, cơ quan chủ quản hệ thống thông tin quan trọng về an ninh quốc gia, các doanh nghiệp cung cấp dịch vụ viễn thông, internet trong và ngoài nước, các chuyên gia hàng đầu về pháp luật, công nghệ thông tin, an toàn thông tin, an ninh mạng, các cơ quan thông tấn, báo chí.

Dự án Luật An ninh mạng đã được tổ chức lấy ý kiến bằng văn bản của các bộ, ngành, Ủy ban nhân dân các tỉnh, thành phố trực thuộc trung ương, các doanh nghiệp cung cấp dịch vụ viễn thông, internet và lấy ý kiến đóng góp của toàn xã hội trên Cổng thông tin điện tử Chính phủ, Trang thông tin điện tử của Bộ Công an, Bộ Tư pháp.

Đồng thời, Bộ Công an cũng tổ chức làm việc với Bộ Tư pháp, Văn phòng Chính phủ, Bộ Thông tin và Truyền thông về nội dung chi tiết của dự án Luật An ninh mạng; tiếp và làm việc với hàng trăm đoàn công tác của cơ quan, tổ chức, doanh nghiệp trong và ngoài nước quan tâm tới nội dung Luật An ninh mạng.

Trên cơ sở dự thảo được Ban soạn thảo xây dựng, Bộ Tư pháp đã thẩm định theo đúng quy trình ban hành văn bản quy phạm pháp luật hiện hành, Chính phủ đã xem xét tại Phiên họp thường kỳ tháng 7/2017, Ủy ban Quốc phòng và An ninh đã thẩm tra sơ bộ ngày 01/9/2017, ngày 14/9/2017, Ủy ban thường vụ Quốc hội đã cho ý kiến đồng ý trình Quốc hội khóa XIV dự án Luật An ninh mạng.

Ngày 12/6/2018, tại kỳ họp thứ 5, Quốc hội khóa XIV đã thông qua Luật An ninh mạng với tỷ lệ 86,86% đồng ý.

Như vậy, Luật An ninh mạng được chuẩn bị công phu, kỹ lưỡng, với sự tham gia đóng góp ý kiến của các bộ, ngành chức năng, hơn 300 doanh nghiệp viễn thông, công nghệ thông tin lớn trong nước; nhiều chuyên gia, tập đoàn kinh tế, viễn thông trong và ngoài nước, trong đó có Facebook, Google, Apple, Amazon, Hội đồng kinh doanh Hoa Kỳ - ASEAN, Hiệp hội điện toán đám mây châu Á; các cơ quan đại diện nước ngoài như Hoa Kỳ, Canađa, Ôxtrâylia, Nhật Bản... và ý kiến rộng rãi của quần chúng nhân dân.

Là đạo luật liên quan đến nhiều mặt của đời sống xã hội nên quá trình xây dựng Luật An ninh mạng đã nhận được các ý kiến phản biện theo nhiều chiều hướng khác nhau. Một số cơ quan đại diện ngoại giao bày tỏ lo ngại, tác động nội dung của Luật, thậm chí đề nghị hoãn không ban hành

Luật An ninh mạng. Nguyên nhân là vì một số doanh nghiệp cung cấp dịch vụ nước ngoài hiện đang hoạt động tại Việt Nam. Các doanh nghiệp trong nước mong muốn có môi trường kinh doanh bình đẳng, không bị bất bình đẳng với các doanh nghiệp cung cấp dịch vụ nước ngoài. Trong khi đó, các doanh nghiệp cung cấp dịch vụ nước ngoài tiếp tục muốn duy trì lợi thế về công nghệ, tài chính để chiếm lĩnh thị trường Việt Nam nên đã tăng cường các hoạt động tiếp xúc đối ngoại, góp ý dự thảo, tác động dư luận đối với nội dung dự thảo Luật An ninh mạng. Hầu hết quần chúng nhân dân đều nhận thức được nguy cơ từ không gian mạng nên đã ủng hộ các quy định nhằm xây dựng một không gian mạng lành mạnh. Tuy nhiên, cũng có một bộ phận quần chúng nhân dân do chưa nắm bắt được nội dung của Luật An ninh mạng, tin vào những luận điệu tuyên truyền sai sự thật trên mạng internet có những băn khoăn về khả năng không được tham gia mạng internet, không được buôn bán trên mạng. Các thế lực thù địch, phản động, chống đối đã có những hoạt động chống phá quyết liệt nội dung Luật An ninh mạng, không chỉ xuyên tạc, bịa đặt nội dung về Luật An ninh mạng, vu cáo vi phạm dân chủ, nhân quyền, số đối tượng này còn kích động biểu tình, gây rối an ninh trật tự. Từ những ý kiến nêu trên, để bảo đảm lợi ích quốc gia, dân tộc cũng như phát huy quyền và lợi ích của Nhân dân,

Đảng, Nhà nước ta thực hiện quan điểm rõ ràng và nhất quán là giải quyết theo hướng vừa bảo đảm yêu cầu quản lý nhà nước nhưng không làm rào cản cho phát triển kinh tế, xã hội.

IV. BỐ CỤC CỦA LUẬT

Luật An ninh mạng năm 2018 gồm 7 chương, 43 điều, quy định những nội dung cơ bản về bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia; phòng ngừa, xử lý hành vi xâm phạm an ninh mạng; triển khai hoạt động bảo vệ an ninh mạng và quy định trách nhiệm của cơ quan, tổ chức, cá nhân. Bố cục của Luật cụ thể như sau:

Chương I. Những quy định chung, gồm 9 điều (từ Điều 1 đến Điều 9) quy định về phạm vi điều chỉnh; giải thích từ ngữ; chính sách của Nhà nước về an ninh mạng; nguyên tắc bảo vệ an ninh mạng; biện pháp bảo vệ an ninh mạng; bảo vệ không gian mạng quốc gia; hợp tác quốc tế về an ninh mạng; các hành vi bị nghiêm cấm về an ninh mạng; xử lý vi phạm pháp luật về an ninh mạng.

Chương II. Bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia, gồm 6 điều (từ Điều 10 đến Điều 15) quy định về hệ thống thông tin quan trọng về an ninh quốc gia; thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia;

đánh giá điều kiện an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia; kiểm tra an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia; giám sát an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia; ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia.

Chương III. Phòng ngừa, xử lý hành vi xâm phạm an ninh mạng, gồm 7 điều (từ Điều 16 đến Điều 22) quy định về phòng ngừa, xử lý thông tin trên không gian mạng có nội dung tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam; kích động gây bạo loạn, phá rối an ninh, gây rối trật tự công cộng; làm nhục, vu khống; xâm phạm trật tự quản lý kinh tế; phòng, chống gián điệp mạng; bảo vệ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên không gian mạng; phòng, chống hành vi sử dụng không gian mạng, công nghệ thông tin, phương tiện điện tử để vi phạm pháp luật về an ninh quốc gia, trật tự, an toàn xã hội; phòng, chống tấn công mạng; phòng, chống khủng bố mạng; phòng ngừa, xử lý tình huống nguy hiểm về an ninh mạng; đấu tranh bảo vệ an ninh mạng.

Chương IV. Hoạt động bảo vệ an ninh mạng, gồm 7 điều (từ Điều 23 đến Điều 29) quy

định về triển khai hoạt động bảo vệ an ninh mạng trong cơ quan nhà nước, tổ chức chính trị ở trung ương và địa phương; kiểm tra an ninh mạng đối với hệ thống thông tin của cơ quan, tổ chức không thuộc Danh mục hệ thống thông tin quan trọng về an ninh quốc gia; bảo vệ an ninh mạng đối với cơ sở hạ tầng không gian mạng quốc gia; cổng kết nối mạng quốc tế; bảo đảm an ninh thông tin trên không gian mạng; nghiên cứu, phát triển an ninh mạng; nâng cao năng lực tự chủ về an ninh mạng; bảo vệ trẻ em trên không gian mạng.

Chương V. Bảo đảm hoạt động bảo vệ an ninh mạng, gồm 6 điều (từ Điều 30 đến Điều 35) quy định về lực lượng bảo vệ an ninh mạng; bảo đảm nguồn nhân lực bảo vệ an ninh mạng; tuyển chọn, đào tạo, phát triển lực lượng bảo vệ an ninh mạng; giáo dục, bồi dưỡng kiến thức, nghiệp vụ an ninh mạng; phổ biến kiến thức về an ninh mạng; kinh phí bảo vệ an ninh mạng.

Chương VI. Trách nhiệm của cơ quan, tổ chức, cá nhân, gồm 7 điều (từ Điều 36 đến Điều 42) quy định về trách nhiệm của Bộ Công an; trách nhiệm của Bộ Quốc phòng; trách nhiệm của Bộ Thông tin và Truyền thông; trách nhiệm của Ban Cơ yếu Chính phủ; trách nhiệm của các bộ, ngành, Ủy ban nhân dân cấp tỉnh; trách nhiệm của doanh nghiệp cung cấp dịch vụ trên không gian mạng; trách nhiệm của cơ quan, tổ chức, cá nhân sử dụng không gian mạng.

Chương VII. Điều khoản thi hành, gồm 01 điều (Điều 43), theo đó, Luật An ninh mạng năm 2018 có hiệu lực thi hành từ ngày 01/01/2019.

Luật An ninh mạng năm 2018 được ban hành góp phần nâng cao hiệu quả công tác bảo vệ chủ quyền, lợi ích, an ninh quốc gia, quyền và lợi ích hợp pháp của tổ chức, cá nhân tham gia hoạt động trên không gian mạng, xây dựng môi trường không gian mạng lành mạnh. Tạo hành lang pháp lý vững chắc, ổn định để các lực lượng chức năng có liên quan có thể áp dụng, triển khai một cách đồng bộ, thống nhất, có cơ sở đấu tranh với hoạt động sử dụng không gian mạng vi phạm pháp luật. Nâng cao khả năng bảo vệ an ninh mạng đối với hệ thống thông tin, nhất là hệ thống thông tin quan trọng về an ninh quốc gia trước những nguy cơ đến từ không gian mạng, đảm bảo hiệu quả công tác quản lý nhà nước trong lĩnh vực này.

Luật An ninh mạng năm 2018 là văn bản mang tính chính sách đầu tiên về nâng cao năng lực tự chủ về an ninh mạng, hoàn thiện chính sách nghiên cứu, phát triển chiến lược về an ninh mạng. Công dân đã được trao những công cụ pháp lý quan trọng để bảo vệ thông tin cá nhân trên không gian mạng; trẻ em được quyền truy cập, tham gia hoạt động trên không gian mạng nhưng cũng là chủ thể được bảo vệ đặc biệt trước các thông tin xấu, độc, không phù hợp với môi trường, văn hóa Việt Nam. Doanh nghiệp, tổ chức trong

và ngoài nước được bình đẳng về nghĩa vụ, trách nhiệm và quyền lợi, bước đầu giải quyết được thực trạng doanh nghiệp trong nước chịu nhiều trách nhiệm pháp lý hơn các doanh nghiệp cung cấp dịch vụ xuyên biên giới. Nhiều quy định trong Luật An ninh mạng năm 2018 quy định rõ trách nhiệm với cộng đồng của các cơ quan, tổ chức, doanh nghiệp trong quản lý hệ thống thông tin và cung cấp dịch vụ trên không gian mạng. Một khi các trách nhiệm này được thực hiện sẽ góp phần quan trọng hình thành không gian mạng an toàn, lành mạnh tạo điều kiện thúc đẩy ổn định chính trị, phát triển kinh tế số của Việt Nam.

Phần II

NHỮNG NỘI DUNG CƠ BẢN CỦA LUẬT AN NINH MẠNG NĂM 2018

I. NHỮNG QUY ĐỊNH CHUNG

1. Về phạm vi điều chỉnh

Luật An ninh mạng năm 2018 quy định về hoạt động bảo vệ an ninh quốc gia và bảo đảm trật tự, an toàn xã hội trên không gian mạng; trách nhiệm của cơ quan, tổ chức, cá nhân có liên quan.

2. Về giải thích từ ngữ: Lần đầu tiên 14 thuật ngữ được định nghĩa và luật hóa, trong đó, có những từ, cụm từ rất quan trọng; cụ thể như:

- *An ninh mạng* là sự bảo đảm hoạt động trên không gian mạng không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

- *Bảo vệ an ninh mạng* là phòng ngừa, phát hiện, ngăn chặn, xử lý hành vi xâm phạm an ninh mạng.

- *Không gian mạng* là mạng lưới kết nối của cơ sở hạ tầng công nghệ thông tin, bao gồm mạng

viễn thông, mạng internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu; là nơi con người thực hiện các hành vi xã hội không bị giới hạn bởi không gian và thời gian.

- *Không gian mạng quốc gia* là không gian mạng do Chính phủ xác lập, quản lý và kiểm soát.

- *Cơ sở hạ tầng không gian mạng quốc gia* là hệ thống cơ sở vật chất, kỹ thuật để tạo lập, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin trên không gian mạng quốc gia bao gồm:

+ Hệ thống truyền dẫn bao gồm hệ thống truyền dẫn quốc gia, hệ thống truyền dẫn kết nối quốc tế, hệ thống vệ tinh, hệ thống truyền dẫn của doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng internet và các dịch vụ gia tăng trên không gian mạng;

+ Hệ thống các dịch vụ lõi bao gồm hệ thống phân luồng và điều hướng thông tin quốc gia, hệ thống phân giải tên miền quốc gia (DNS), hệ thống chứng thực quốc gia (PKI/CA) và hệ thống cung cấp dịch vụ kết nối, truy cập internet của doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng internet và các dịch vụ gia tăng trên không gian mạng;

+ Dịch vụ, ứng dụng công nghệ thông tin bao gồm dịch vụ trực tuyến; ứng dụng công nghệ thông tin có kết nối mạng phục vụ quản lý, điều

hành của cơ quan, tổ chức, tập đoàn kinh tế, tài chính quan trọng; cơ sở dữ liệu quốc gia.

Dịch vụ trực tuyến bao gồm chính phủ điện tử, thương mại điện tử, trang thông tin điện tử, diễn đàn trực tuyến, mạng xã hội, blog;

+ Cơ sở hạ tầng công nghệ thông tin của đô thị thông minh, internet vạn vật, hệ thống phức hợp thực - ảo, điện toán đám mây, hệ thống dữ liệu lớn, hệ thống dữ liệu nhanh và hệ thống trí tuệ nhân tạo.

- *Cổng kết nối mạng quốc tế* là nơi diễn ra hoạt động chuyển nhận tín hiệu mạng qua lại giữa Việt Nam và các quốc gia, vùng lãnh thổ khác.

- *Tội phạm mạng* là hành vi sử dụng không gian mạng, công nghệ thông tin hoặc phương tiện điện tử để thực hiện tội phạm được quy định tại Bộ luật Hình sự.

- *Tấn công mạng* là hành vi sử dụng không gian mạng, công nghệ thông tin hoặc phương tiện điện tử để phá hoại, gây gián đoạn hoạt động của mạng viễn thông, mạng internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử.

- *Khủng bố mạng* là việc sử dụng không gian mạng, công nghệ thông tin hoặc phương tiện điện tử để thực hiện hành vi khủng bố, tài trợ khủng bố.

- *Gián điệp mạng* là hành vi cố ý vượt qua cảnh báo, mã truy cập, mật mã, tường lửa, sử

dụng quyền quản trị của người khác hoặc bằng phương thức khác để chiếm đoạt, thu thập trái phép thông tin, tài nguyên thông tin trên mạng viễn thông, mạng internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu hoặc phương tiện điện tử của cơ quan, tổ chức, cá nhân.

- *Tài khoản số* là thông tin dùng để chứng thực, xác thực, phân quyền sử dụng các ứng dụng, dịch vụ trên không gian mạng.

- *Nguy cơ đe dọa an ninh mạng* là tình trạng không gian mạng xuất hiện dấu hiệu đe dọa xâm phạm an ninh quốc gia, gây tổn hại nghiêm trọng trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

- *Sự cố an ninh mạng* là sự việc bất ngờ xảy ra trên không gian mạng xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

- *Tình huống nguy hiểm về an ninh mạng* là sự việc xảy ra trên không gian mạng khi có hành vi xâm phạm nghiêm trọng an ninh quốc gia, gây tổn hại đặc biệt nghiêm trọng trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

3. Về chính sách của Nhà nước về an ninh mạng

Quốc hội khóa XIV thông qua Luật An ninh

mạng năm 2018 đã góp phần hoàn thiện cơ bản hệ thống pháp luật về an ninh mạng - Nhà nước ta đã có đạo luật riêng quy định về hoạt động bảo vệ an ninh quốc gia và bảo đảm trật tự, an toàn xã hội trên không gian mạng; trách nhiệm của cơ quan, tổ chức, cá nhân có liên quan, nhất là các quy định về hệ thống thông tin quan trọng về an ninh quốc gia, tấn công mạng, gián điệp mạng, tình báo mạng, khủng bố mạng, bảo đảm lợi ích quốc gia trên không gian mạng; giải quyết được những hạn chế thời gian qua như: vấn đề an ninh mạng chưa được điều chỉnh hoặc tuy có được quy định nhưng chủ yếu bằng các quy định dưới luật nên hiệu lực pháp lý thấp, kết quả thực hiện không cao; nhiều quy định trong các văn bản về an ninh mạng còn chưa phù hợp với thực tế, thiếu tính khả thi; một số quy định mới được thực hiện đã có nhu cầu cần sửa đổi, bổ sung.

Điều 3 Luật An ninh mạng năm 2018 quy định: (1) Ưu tiên, bảo vệ an ninh mạng trong quốc phòng, an ninh, phát triển kinh tế - xã hội, khoa học, công nghệ và đối ngoại; (2) Xây dựng không gian mạng lành mạnh, không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân; (3) Ưu tiên nguồn lực xây dựng lực lượng chuyên trách bảo vệ an ninh mạng; nâng cao năng lực cho lực lượng bảo vệ an ninh mạng và tổ chức, cá nhân tham gia bảo vệ an ninh mạng;

ưu tiên đầu tư cho nghiên cứu, phát triển khoa học, công nghệ để bảo vệ an ninh mạng; (4) Khuyến khích, tạo điều kiện để tổ chức, cá nhân tham gia bảo vệ an ninh mạng, xử lý các nguy cơ đe dọa an ninh mạng; nghiên cứu, phát triển công nghệ, sản phẩm, dịch vụ, ứng dụng nhằm bảo vệ an ninh mạng; phối hợp với cơ quan chức năng trong bảo vệ an ninh mạng; (5) Tăng cường hợp tác quốc tế về an ninh mạng.

4. Về nguyên tắc bảo vệ an ninh mạng

Luật An ninh mạng năm 2018 quy định việc bảo vệ an ninh mạng phải tuân thủ 07 nguyên tắc sau: (1) Tuân thủ Hiến pháp và pháp luật; bảo đảm lợi ích của Nhà nước, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân; (2) Đặt dưới sự lãnh đạo của Đảng Cộng sản Việt Nam, sự quản lý thống nhất của Nhà nước; huy động sức mạnh tổng hợp của hệ thống chính trị và toàn dân tộc; phát huy vai trò nòng cốt của lực lượng chuyên trách bảo vệ an ninh mạng; (3) Kết hợp chặt chẽ giữa nhiệm vụ bảo vệ an ninh mạng, bảo vệ hệ thống thông tin quan trọng về an ninh quốc gia với nhiệm vụ phát triển kinh tế - xã hội, bảo đảm quyền con người, quyền công dân, tạo điều kiện cho cơ quan, tổ chức, cá nhân hoạt động trên không gian mạng; (4) Chủ động phòng ngừa, phát hiện, ngăn chặn, đấu tranh, làm thất bại mọi hoạt động sử dụng không gian mạng xâm phạm

an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân; sẵn sàng ngăn chặn các nguy cơ đe dọa an ninh mạng; (5) Triển khai hoạt động bảo vệ an ninh mạng đối với cơ sở hạ tầng không gian mạng quốc gia; áp dụng các biện pháp bảo vệ hệ thống thông tin quan trọng về an ninh quốc gia; (6) Hệ thống thông tin quan trọng về an ninh quốc gia được thẩm định, chứng nhận đủ điều kiện về an ninh mạng trước khi đưa vào vận hành, sử dụng; thường xuyên kiểm tra, giám sát về an ninh mạng trong quá trình sử dụng và kịp thời ứng phó, khắc phục sự cố an ninh mạng; (7) Mọi hành vi vi phạm pháp luật về an ninh mạng phải được xử lý kịp thời, nghiêm minh.

5. Về biện pháp bảo vệ an ninh mạng

Luật quy định chi tiết, cụ thể các biện pháp bảo vệ an ninh mạng. Đây là những biện pháp hành chính, kỹ thuật chung, vừa bảo vệ an ninh quốc gia, trật tự, an toàn xã hội, vừa bảo vệ quyền và lợi ích hợp pháp của tổ chức, cá nhân trên không gian mạng. Khoản 1 Điều 5 Luật An ninh mạng năm 2018 quy định các biện pháp bảo vệ an ninh mạng bao gồm: (1) Thẩm định an ninh mạng; (2) Đánh giá điều kiện an ninh mạng; (3) Kiểm tra an ninh mạng; (4) Giám sát an ninh mạng; (5) Ứng phó, khắc phục sự cố an ninh mạng; (6) Đấu tranh, bảo vệ an ninh mạng; (7) Sử dụng mật mã

để bảo vệ thông tin mạng; (8) Ngăn chặn, yêu cầu tạm ngừng, ngừng cung cấp thông tin mạng; đình chỉ, tạm đình chỉ các hoạt động thiết lập, cung cấp và sử dụng mạng viễn thông, mạng internet, sản xuất và sử dụng thiết bị phát, thu phát sóng vô tuyến theo quy định của pháp luật; (9) Yêu cầu xóa bỏ, truy cập xóa bỏ thông tin trái pháp luật hoặc thông tin quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân trên không gian mạng; (10) Phong tỏa, hạn chế hoạt động của hệ thống thông tin; đình chỉ, tạm đình chỉ hoặc yêu cầu ngừng hoạt động của hệ thống thông tin, thu hồi tên miền theo quy định của pháp luật; (11) Khởi tố, điều tra, truy tố, xét xử theo quy định của Bộ luật Tố tụng hình sự; (12) Biện pháp khác theo quy định của pháp luật về an ninh quốc gia, pháp luật về xử lý vi phạm hành chính.

Bên cạnh đó, Luật giao Chính phủ quy định trình tự, thủ tục áp dụng biện pháp bảo vệ an ninh mạng, trừ biện pháp khởi tố, điều tra, truy tố, xét xử theo quy định của Bộ luật Tố tụng hình sự và biện pháp khác theo quy định của pháp luật về an ninh quốc gia, pháp luật về xử lý vi phạm hành chính.

6. Về hợp tác quốc tế về an ninh mạng

Luật An ninh mạng năm 2018 quy định hợp tác quốc tế về an ninh mạng được thực hiện trên

cơ sở tôn trọng độc lập, chủ quyền và toàn vẹn lãnh thổ, không can thiệp vào công việc nội bộ của nhau, bình đẳng và cùng có lợi (khoản 1 Điều 7). Trên cơ sở đó, Luật quy định cụ thể nội dung hợp tác quốc tế về an ninh mạng (khoản 2 Điều 7), đồng thời giao Bộ Công an chịu trách nhiệm trước Chính phủ chủ trì, phối hợp thực hiện hợp tác quốc tế về an ninh mạng, trừ hoạt động hợp tác quốc tế của Bộ Quốc phòng; Bộ Quốc phòng chịu trách nhiệm trước Chính phủ thực hiện hợp tác quốc tế về an ninh mạng trong phạm vi quản lý; Bộ Ngoại giao có trách nhiệm phối hợp với Bộ Công an, Bộ Quốc phòng trong hoạt động hợp tác quốc tế về an ninh mạng; trường hợp hợp tác quốc tế về an ninh mạng có liên quan đến trách nhiệm của nhiều bộ, ngành do Chính phủ quyết định (khoản 3 Điều 7).

Bên cạnh đó, Luật quy định hoạt động hợp tác quốc tế về an ninh mạng của bộ, ngành khác, của địa phương phải có văn bản tham gia ý kiến của Bộ Công an trước khi triển khai, trừ hoạt động hợp tác quốc tế của Bộ Quốc phòng (khoản 4 Điều 7).

7. Các hành vi bị nghiêm cấm về an ninh mạng

Luật An ninh mạng năm 2018 chỉ nghiêm cấm sử dụng không gian mạng để thực hiện các hành vi vi phạm pháp luật đã được pháp luật (Bộ luật

Hình sự, Bộ luật Dân sự và các văn bản quy phạm pháp luật khác liên quan) quy định. Theo đó, Điều 8 Luật An ninh mạng năm 2018 đã liệt kê cụ thể, rõ ràng các hành vi bị nghiêm cấm về an ninh mạng, góp phần thuận lợi trong việc thực hiện và xử lý hành vi vi phạm điều cấm, bao gồm: (1) Sử dụng không gian mạng để thực hiện hành vi sau đây: (a) Hành vi quy định tại khoản 1 Điều 18 Luật An ninh mạng năm 2018; (b) Tổ chức, hoạt động, câu kết, xúi giục, mua chuộc, lừa gạt, lôi kéo, đào tạo, huấn luyện người chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam; (c) Xuyên tạc lịch sử, phủ nhận thành tựu cách mạng, phá hoại khối đại đoàn kết toàn dân tộc, xúc phạm tôn giáo, phân biệt đối xử về giới, phân biệt chủng tộc; (d) Thông tin sai sự thật gây hoang mang trong Nhân dân, gây thiệt hại cho hoạt động kinh tế - xã hội, gây khó khăn cho hoạt động của cơ quan nhà nước hoặc người thi hành công vụ, xâm phạm quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác; (đ) Hoạt động mại dâm, tệ nạn xã hội, mua bán người; đăng tải thông tin dâm ô, đồi trụy, tội ác; phá hoại thuần phong, mỹ tục của dân tộc, đạo đức xã hội, sức khỏe của cộng đồng; (e) Xúi giục, lôi kéo, kích động người khác phạm tội; (2) Thực hiện tấn công mạng, khủng bố mạng, gián điệp mạng, tội phạm mạng; gây sự cố, tấn công, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt hoặc phá hoại hệ thống

thông tin quan trọng về an ninh quốc gia; (3) Sản xuất, đưa vào sử dụng công cụ, phương tiện, phần mềm hoặc có hành vi cản trở, gây rối loạn hoạt động của mạng viễn thông, mạng internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, phương tiện điện tử; phát tán chương trình tin học gây hại cho hoạt động của mạng viễn thông, mạng internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, phương tiện điện tử; xâm nhập trái phép vào mạng viễn thông, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử của người khác; (4) Chống lại hoặc cản trở hoạt động của lực lượng bảo vệ an ninh mạng; tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng biện pháp bảo vệ an ninh mạng; (5) Lợi dụng hoặc lạm dụng hoạt động bảo vệ an ninh mạng để xâm phạm chủ quyền, lợi ích, an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân hoặc để trục lợi; (6) Hành vi khác vi phạm quy định của Luật An ninh mạng năm 2018.

Như vậy, Luật An ninh mạng năm 2018 không có quy định cấm Facebook, Google hoặc các nhà cung cấp dịch vụ nước ngoài hoạt động tại Việt Nam; không ngăn cản quyền tự do ngôn luận, quyền bày tỏ quan điểm của công dân; không cấm công dân sử dụng các dịch vụ mạng xã hội như

Facebook, Google; không cấm công dân tham gia hoạt động trên không gian mạng hoặc truy cập, sử dụng thông tin trên không gian mạng; cấm công dân khởi nghiệp, sáng tạo hay trao đổi, triển khai ý tưởng sáng tạo của mình trên không gian mạng.

8. Xử lý vi phạm pháp luật về an ninh mạng

Bên cạnh việc quy định các hành vi bị nghiêm cấm, Luật An ninh mạng năm 2018 có quy định về xử lý vi phạm pháp luật về an ninh mạng tại Điều 9. Theo đó, người nào có hành vi vi phạm quy định của Luật An ninh mạng năm 2018 thì tùy theo tính chất, mức độ vi phạm mà bị xử lý kỷ luật, xử lý vi phạm hành chính hoặc bị truy cứu trách nhiệm hình sự, nếu gây thiệt hại thì phải bồi thường theo quy định của pháp luật.

II. BẢO VỆ AN NINH MẠNG ĐỐI VỚI HỆ THỐNG THÔNG TIN QUAN TRỌNG VỀ AN NINH QUỐC GIA

Quy định bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia là một trong những nội dung đặc biệt quan trọng của Luật An ninh mạng năm 2018, quy định về hệ thống thông tin quan trọng về an ninh quốc gia và thể hiện đầy đủ các biện pháp, hoạt động bảo vệ tương xứng với mức độ quan trọng của hệ thống

thông tin, trong đó nêu ra tiêu chí xác định, lĩnh vực liên quan, quy định các biện pháp như thẩm định an ninh mạng, đánh giá điều kiện, kiểm tra, giám sát an ninh mạng và ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia.

1. Về hệ thống thông tin quan trọng về an ninh quốc gia

Hệ thống thông tin quan trọng về an ninh quốc gia được hiểu là hệ thống thông tin khi bị sự cố, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt, tấn công hoặc phá hoại sẽ xâm phạm nghiêm trọng an ninh mạng (khoản 1 Điều 10).

Hệ thống thông tin quan trọng về an ninh quốc gia được xác định trong các lĩnh vực đặc biệt quan trọng đối với quốc gia hay trong lĩnh vực đặc thù, bao gồm: (1) Hệ thống thông tin quân sự, an ninh, ngoại giao, cơ yếu; (2) Hệ thống thông tin lưu trữ, xử lý thông tin thuộc bí mật nhà nước; (3) Hệ thống thông tin phục vụ lưu giữ, bảo quản hiện vật, tài liệu có giá trị đặc biệt quan trọng; (4) Hệ thống thông tin phục vụ bảo quản, chế tạo, quản lý cơ sở vật chất đặc biệt quan trọng khác liên quan đến an ninh quốc gia; (5) Hệ thống thông tin bảo quản, chế tạo, quản lý cơ sở vật chất đặc biệt quan trọng khác liên quan đến an ninh quốc gia; (6) Hệ thống thông tin quan trọng phục vụ hoạt

động của cơ quan, tổ chức ở trung ương; (7) Hệ thống thông tin quốc gia thuộc lĩnh vực năng lượng, tài chính, ngân hàng, viễn thông, giao thông vận tải, tài nguyên và môi trường, hóa chất, y tế, văn hóa, báo chí; (8) Hệ thống điều khiển và giám sát tự động tại công trình quan trọng liên quan đến an ninh quốc gia, mục tiêu quan trọng về an ninh quốc gia (khoản 2 Điều 10).

Luật An ninh mạng năm 2018 quy định Thủ tướng Chính phủ ban hành và sửa đổi, bổ sung Danh mục hệ thống thông tin quan trọng về an ninh quốc gia (khoản 3 Điều 10). Đồng thời, để tạo thuận lợi cho các chủ quản hệ thống thông tin trong việc thực hiện các nội dung quản lý nhà nước có liên quan đến thẩm quyền của nhiều bộ khác nhau, Luật giao Chính phủ quy định việc phối hợp giữa các bộ, ngành chức năng trong việc thẩm định, đánh giá, kiểm tra, giám sát, ứng phó, khắc phục sự cố đối với hệ thống thông tin quan trọng về an ninh quốc gia (khoản 4 Điều 10).

2. Về thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia

Thẩm định an ninh mạng là hoạt động xem xét, đánh giá những nội dung về an ninh mạng để làm cơ sở cho việc quyết định xây dựng hoặc nâng cấp hệ thống thông tin (khoản 1 Điều 11).

Hoạt động thẩm định an ninh mạng do lực lượng chuyên trách bảo vệ an ninh mạng thực hiện, áp dụng đối với hệ thống thông tin quan trọng về an ninh quốc gia. Đây là những hệ thống thông tin thuộc các bộ, ban, ngành, tập đoàn, doanh nghiệp của Nhà nước, có vị trí, vai trò, tầm quan trọng đối với an ninh quốc gia, cần được bảo vệ bằng biện pháp tương xứng. Chủ quản hệ thống thông tin quan trọng về an ninh quốc gia phải bảo đảm cho hệ thống của mình đáp ứng các nội dung thẩm định để làm cơ sở cho việc quyết định xây dựng hoặc nâng cấp hệ thống thông tin.

Về đối tượng thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia bao gồm: a) Báo cáo nghiên cứu tiền khả thi, hồ sơ thiết kế thi công dự án đầu tư xây dựng hệ thống thông tin trước khi phê duyệt; b) Đề án nâng cấp hệ thống thông tin trước khi phê duyệt (khoản 2 Điều 11).

Về nội dung thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia bao gồm: a) Việc tuân thủ quy định, điều kiện an ninh mạng trong thiết kế; b) Sự phù hợp với phương án bảo vệ, ứng phó, khắc phục sự cố và bố trí nhân lực bảo vệ an ninh mạng (khoản 3 Điều 11).

Về thẩm quyền thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh

quốc gia bao gồm: a) Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia, trừ trường hợp quy định tại điểm b và điểm c khoản 4 Điều 11 Luật An ninh mạng năm 2018; b) Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng thẩm định an ninh mạng đối với hệ thống thông tin quân sự; c) Ban Cơ yếu Chính phủ thẩm định an ninh mạng đối với hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ (khoản 4 Điều 11).

3. Về đánh giá điều kiện an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia

Luật An ninh mạng năm 2018 quy định về đánh giá điều kiện về an ninh mạng là hoạt động xem xét sự đáp ứng về an ninh mạng của hệ thống thông tin trước khi đưa vào vận hành, sử dụng (khoản 1 Điều 12).

Luật quy định cụ thể các điều kiện của hệ thống thông tin quan trọng về an ninh quốc gia tại khoản 2 Điều 12, bao gồm: a) Quy định, quy trình và phương án bảo đảm an ninh mạng; nhân sự vận hành, quản trị hệ thống; b) Bảo đảm an ninh mạng đối với trang thiết bị, phần cứng, phần mềm là thành phần hệ thống; c) Biện pháp kỹ thuật để giám sát, bảo vệ an ninh mạng; biện pháp bảo vệ hệ thống điều khiển và giám sát

tự động, internet vạn vật, hệ thống phức hợp thực - ảo, điện toán đám mây, hệ thống dữ liệu lớn, hệ thống dữ liệu nhanh, hệ thống trí tuệ nhân tạo; d) Biện pháp bảo đảm an ninh vật lý bao gồm cách ly cô lập đặc biệt, chống rò rỉ dữ liệu, chống thu tin, kiểm soát ra vào.

Luật An ninh mạng năm 2018 quy định thẩm quyền đánh giá điều kiện an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia cho lực lượng chuyên trách bảo vệ an ninh mạng thuộc các Bộ Công an, Bộ Quốc phòng, Ban Cơ yếu Chính phủ (khoản 3 Điều 12). Theo đó, Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng đánh giá, chứng nhận đủ điều kiện an ninh mạng đối với hệ thống thông tin quân sự; Ban Cơ yếu Chính phủ đánh giá, chứng nhận đủ điều kiện an ninh mạng đối với hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ; Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an đánh giá, chứng nhận đủ điều kiện an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia, trừ trường hợp do Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng, Ban Cơ yếu Chính phủ đánh giá, chứng nhận.

Đồng thời, Luật quy định hệ thống thông tin quan trọng về an ninh quốc gia được đưa vào vận hành, sử dụng sau khi được chứng nhận đủ điều kiện an ninh mạng và giao Chính phủ quy định

chi tiết về điều kiện của hệ thống thông tin quan trọng về an ninh quốc gia.

4. Về kiểm tra an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia

Kiểm tra an ninh mạng là hoạt động xác định thực trạng an ninh mạng của hệ thống thông tin, cơ sở hạ tầng hệ thống thông tin hoặc thông tin được lưu trữ, xử lý, truyền đưa trong hệ thống thông tin nhằm phòng ngừa, phát hiện, xử lý nguy cơ đe dọa an ninh mạng và đưa ra các phương án, biện pháp bảo đảm hoạt động bình thường của hệ thống thông tin (khoản 1 Điều 13).

Luật An ninh mạng năm 2018 quy định cụ thể các trường hợp, đối tượng kiểm tra an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia, cụ thể:

- Kiểm tra an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia được thực hiện trong trường hợp sau đây: a) Khi đưa phương tiện điện tử, dịch vụ an toàn thông tin mạng vào sử dụng trong hệ thống thông tin; b) Khi có thay đổi hiện trạng hệ thống thông tin; c) Kiểm tra định kỳ hằng năm; (d) Kiểm tra đột xuất khi xảy ra sự cố an ninh mạng, hành vi xâm phạm an ninh mạng; khi có yêu cầu quản lý nhà nước về an ninh mạng; khi hết thời hạn khắc phục điểm yếu, lỗ hổng bảo mật theo khuyến cáo

của lực lượng chuyên trách bảo vệ an ninh mạng (khoản 2 Điều 13).

- Về đối tượng kiểm tra an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia bao gồm: a) Hệ thống phần cứng, phần mềm, thiết bị số được sử dụng trong hệ thống thông tin; b) Quy định, biện pháp bảo vệ an ninh mạng; c) Thông tin được lưu trữ, xử lý, truyền đưa trong hệ thống thông tin; d) Phương án ứng phó, khắc phục sự cố an ninh mạng của chủ quản hệ thống thông tin; đ) Biện pháp bảo vệ bí mật nhà nước và phòng, chống lộ, mất bí mật nhà nước qua các kênh kỹ thuật; e) Nhân lực bảo vệ an ninh mạng (khoản 3 Điều 13).

Tuy nhiên, tại khoản 4 Điều 13, Luật An ninh mạng năm 2018 quy định trách nhiệm kiểm tra an ninh mạng đối với hệ thống thông tin thuộc phạm vi quản lý khi đưa phương tiện điện tử, dịch vụ an toàn thông tin mạng vào sử dụng trong hệ thống thông tin; khi có thay đổi hiện trạng hệ thống thông tin và kiểm tra định kỳ hằng năm là do chủ quản hệ thống thông tin quan trọng về an ninh quốc gia và thông báo kết quả kiểm tra bằng văn bản cho lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an hoặc lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng đối với hệ thống thông tin quân sự trước tháng 10 hằng năm.

Cùng đó, tại khoản 5 Điều 13 quy định về việc kiểm tra an ninh mạng đột xuất đối với hệ thống thông tin quan trọng về an ninh quốc gia, cụ thể như sau:

a) Trước thời điểm tiến hành kiểm tra, lực lượng chuyên trách bảo vệ an ninh mạng có trách nhiệm thông báo bằng văn bản cho chủ quản hệ thống thông tin ít nhất là 12 giờ trong trường hợp xảy ra sự cố an ninh mạng, hành vi xâm phạm an ninh mạng; ít nhất là 72 giờ trong trường hợp có yêu cầu quản lý nhà nước về an ninh mạng hoặc hết thời hạn khắc phục điểm yếu, lỗ hổng bảo mật theo khuyến cáo của lực lượng chuyên trách bảo vệ an ninh mạng;

b) Trong thời hạn 30 ngày kể từ ngày kết thúc kiểm tra, lực lượng chuyên trách bảo vệ an ninh mạng thông báo kết quả kiểm tra và đưa ra yêu cầu đối với chủ quản hệ thống thông tin trong trường hợp phát hiện điểm yếu, lỗ hổng bảo mật; hướng dẫn hoặc tham gia khắc phục khi có đề nghị của chủ quản hệ thống thông tin;

c) Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an kiểm tra an ninh mạng đột xuất đối với hệ thống thông tin quan trọng về an ninh quốc gia, trừ hệ thống thông tin quân sự do Bộ Quốc phòng quản lý, hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ và sản phẩm mật mã do Ban Cơ yếu Chính phủ cung cấp để bảo vệ thông tin thuộc bí mật nhà nước.

Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng kiểm tra an ninh mạng đột xuất đối với hệ thống thông tin quân sự.

Ban Cơ yếu Chính phủ kiểm tra an ninh mạng đột xuất đối với hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ và sản phẩm mật mã do Ban Cơ yếu Chính phủ cung cấp để bảo vệ thông tin thuộc bí mật nhà nước;

d) Chủ quản hệ thống thông tin quan trọng về an ninh quốc gia có trách nhiệm phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng tiến hành kiểm tra an ninh mạng đột xuất.

5. Về giám sát an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia

Giám sát an ninh mạng là hoạt động thu thập, phân tích tình hình nhằm xác định nguy cơ đe dọa an ninh mạng, sự cố an ninh mạng, điểm yếu, lỗ hổng bảo mật, mã độc, phần cứng độc hại để cảnh báo, khắc phục, xử lý (khoản 1 Điều 14).

Về cơ quan chủ quản và lực lượng chuyên trách thực hiện nhiệm vụ trong hoạt động giám sát an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia, Luật quy định cụ thể như sau: Chủ quản hệ thống thông tin quan trọng về an ninh quốc gia chủ trì, phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng có thẩm quyền thường xuyên thực hiện giám sát an ninh mạng đối với hệ thống thông tin thuộc phạm vi

quản lý; xây dựng cơ chế tự cảnh báo và tiếp nhận cảnh báo về nguy cơ đe dọa an ninh mạng, sự cố an ninh mạng, điểm yếu, lỗ hổng bảo mật, mã độc, phần cứng độc hại và đề ra phương án ứng phó, khắc phục khẩn cấp (khoản 2 Điều 14). Cùng đó, Luật quy định về lực lượng chuyên trách bảo vệ an ninh mạng thực hiện giám sát an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia thuộc phạm vi quản lý; cảnh báo và phối hợp với chủ quản hệ thống thông tin trong khắc phục, xử lý các nguy cơ đe dọa an ninh mạng, sự cố an ninh mạng, điểm yếu, lỗ hổng bảo mật, mã độc, phần cứng độc hại xảy ra đối với hệ thống thông tin quan trọng về an ninh quốc gia (khoản 3 Điều 14).

6. Ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia

Để ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia, Luật An ninh mạng năm 2018 quy định cụ thể các hoạt động này tại khoản 1 Điều 15 như sau: a) Phát hiện, xác định sự cố an ninh mạng; b) Bảo vệ hiện trường, thu thập chứng cứ; c) Phong tỏa, giới hạn phạm vi xảy ra sự cố an ninh mạng, hạn chế thiệt hại do sự cố an ninh mạng gây ra; d) Xác định mục tiêu, đối tượng, phạm vi cần ứng cứu; đ) Xác minh, phân tích, đánh giá, phân loại

sự cố an ninh mạng; e) Triển khai phương án ứng phó, khắc phục sự cố an ninh mạng; g) Xác minh nguyên nhân và truy tìm nguồn gốc; h) Điều tra, xử lý theo quy định của pháp luật.

Luật quy định việc chủ quản hệ thống thông tin quan trọng sẽ làm gì, phương án nào và phương thức báo cáo với lực lượng chuyên trách bảo vệ an ninh mạng có thẩm quyền khi sự cố an ninh mạng xảy ra đối với hệ thống thông tin thuộc phạm vi quản lý. Bên cạnh đó, việc điều phối hoạt động ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia được giao theo từng lĩnh vực, chức năng, nhiệm vụ, thẩm quyền quản lý nhà nước của Bộ Công an, Bộ Quốc phòng, Ban Cơ yếu Chính phủ và trách nhiệm của cơ quan, tổ chức, cá nhân tham gia ứng phó, khắc phục sự cố an ninh mạng xảy ra đối với hệ thống thông tin quan trọng về an ninh quốc gia khi có yêu cầu của lực lượng chủ trì điều phối, quy định tại khoản 3 và khoản 4 Điều 15.

III. PHÒNG NGỪA, XỬ LÝ HÀNH VI XÂM PHẠM AN NINH MẠNG

Để bảo vệ tối đa quyền và lợi ích hợp pháp của tổ chức, cá nhân, Chương III Luật An ninh mạng năm 2018 quy định đầy đủ các biện pháp phòng ngừa, đấu tranh, xử lý nhằm loại bỏ các nguy cơ

đe dọa, phát hiện và xử lý hành vi vi phạm pháp luật. Đây là hành lang pháp lý vững chắc để người dân có thể yên tâm kinh doanh hay hoạt động trên không gian mạng.

1. Về phòng ngừa, xử lý thông tin trên không gian mạng có nội dung tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam; kích động gây bạo loạn, phá rối an ninh, gây rối trật tự công cộng; làm nhục, vu khống; xâm phạm trật tự quản lý kinh tế

Thông tin trên không gian mạng có nội dung tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam bao gồm: a) Tuyên truyền xuyên tạc, phỉ báng chính quyền nhân dân; b) Chiến tranh tâm lý, kích động chiến tranh xâm lược, chia rẽ, gây thù hận giữa các dân tộc, tôn giáo và nhân dân các nước; c) Xúc phạm dân tộc, quốc kỳ, quốc huy, quốc ca, vĩ nhân, lãnh tụ, danh nhân, anh hùng dân tộc (khoản 1 Điều 16).

Thông tin trên không gian mạng có nội dung kích động gây bạo loạn, phá rối an ninh, gây rối trật tự công cộng bao gồm: a) Kêu gọi, vận động, xúi giục, đe dọa, gây chia rẽ, tiến hành hoạt động vũ trang hoặc dùng bạo lực nhằm chống chính quyền nhân dân; b) Kêu gọi, vận động, xúi giục, đe dọa, lôi kéo tụ tập đông người gây rối, chống người thi hành công vụ, cản trở hoạt động của

cơ quan, tổ chức gây mất ổn định về an ninh, trật tự (khoản 2 Điều 16).

Thông tin trên không gian mạng có nội dung làm nhục, vu khống bao gồm: a) Xúc phạm nghiêm trọng danh dự, uy tín, nhân phẩm của người khác; b) Thông tin bịa đặt, sai sự thật xâm phạm danh dự, uy tín, nhân phẩm hoặc gây thiệt hại đến quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác (khoản 3 Điều 16).

Thông tin trên không gian mạng có nội dung xâm phạm trật tự quản lý kinh tế bao gồm: a) Thông tin bịa đặt, sai sự thật về sản phẩm, hàng hóa, tiền, trái phiếu, tín phiếu, công trái, séc và các loại giấy tờ có giá khác; b) Thông tin bịa đặt, sai sự thật trong lĩnh vực tài chính, ngân hàng, thương mại điện tử, thanh toán điện tử, kinh doanh tiền tệ, huy động vốn, kinh doanh đa cấp, chứng khoán (khoản 4 Điều 16).

Thông tin trên không gian mạng có nội dung bịa đặt, sai sự thật gây hoang mang trong Nhân dân, gây thiệt hại cho hoạt động kinh tế - xã hội, gây khó khăn cho hoạt động của cơ quan nhà nước hoặc người thi hành công vụ, xâm phạm quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác (khoản 5 Điều 16).

Bên cạnh đó, Luật An ninh mạng năm 2018 quy định trách nhiệm của cơ quan chủ quản hệ thống thông tin trong việc triển khai biện pháp

quản lý, kỹ thuật trên hệ thống thông tin thuộc phạm vi quản lý khi có yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng (khoản 6 Điều 16); lực lượng chuyên trách bảo vệ an ninh mạng và cơ quan có thẩm quyền áp dụng biện pháp: ngăn chặn, yêu cầu tạm ngừng, ngừng cung cấp thông tin mạng; đình chỉ, tạm đình chỉ các hoạt động thiết lập, cung cấp và sử dụng mạng viễn thông, mạng internet, sản xuất và sử dụng thiết bị phát, thu phát sóng vô tuyến theo quy định của pháp luật; yêu cầu xóa bỏ, truy cập xóa bỏ thông tin trái pháp luật hoặc thông tin sai sự thật trên không gian mạng xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân; phong tỏa, hạn chế hoạt động của hệ thống thông tin; đình chỉ, tạm đình chỉ hoặc yêu cầu ngừng hoạt động của hệ thống thông tin, thu hồi tên miền theo quy định của pháp luật để xử lý thông tin trên không gian mạng (khoản 7 Điều 16); trách nhiệm của doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng internet, các dịch vụ gia tăng trên không gian mạng và chủ quản hệ thống thông tin (khoản 8 Điều 16) và trách nhiệm của tổ chức, cá nhân đối với thông tin trên không gian mạng (khoản 9 Điều 16).

2. Về phòng, chống gián điệp mạng; bảo vệ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên không gian mạng

Luật An ninh mạng năm 2018 quy định chi tiết các hành vi gián điệp mạng xâm phạm bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên không gian mạng bao gồm: a) Chiếm đoạt, mua bán, thu giữ, cố ý làm lộ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư gây ảnh hưởng đến danh dự, uy tín, nhân phẩm, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân; b) Cố ý xóa, làm hư hỏng, thất lạc, thay đổi thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư được truyền đưa, lưu trữ trên không gian mạng; c) Cố ý thay đổi, hủy bỏ hoặc làm vô hiệu hóa biện pháp kỹ thuật được xây dựng, áp dụng để bảo vệ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư; d) Đưa lên không gian mạng những thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư

trái quy định của pháp luật; đ) Cố ý nghe, ghi âm, ghi hình trái phép các cuộc đàm thoại; e) Hành vi khác cố ý xâm phạm bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư (khoản 1 Điều 17).

Luật quy định chủ quản hệ thống thông tin có trách nhiệm: (1) Kiểm tra an ninh mạng nhằm phát hiện, loại bỏ mã độc, phần cứng độc hại, khắc phục điểm yếu, lỗ hổng bảo mật; phát hiện, ngăn chặn và xử lý các hoạt động xâm nhập bất hợp pháp hoặc nguy cơ khác đe dọa an ninh mạng; (2) Triển khai biện pháp quản lý, kỹ thuật để phòng ngừa, phát hiện, ngăn chặn hành vi gián điệp mạng, xâm phạm bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên hệ thống thông tin và kịp thời gỡ bỏ thông tin liên quan đến hành vi này; (3) Phối hợp, thực hiện yêu cầu của lực lượng chuyên trách an ninh mạng về phòng, chống gián điệp mạng, bảo vệ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên hệ thống thông tin tại khoản 2 Điều 17.

Cơ quan soạn thảo, lưu trữ thông tin, tài liệu thuộc bí mật nhà nước có trách nhiệm bảo vệ bí mật nhà nước được soạn thảo, lưu giữ trên máy tính, thiết bị khác hoặc trao đổi trên không gian

mạng theo quy định của pháp luật về bảo vệ bí mật nhà nước.

Đồng thời, Luật An ninh mạng năm 2018 quy định rất cụ thể trách nhiệm của Bộ Công an, Bộ Quốc phòng và Ban Cơ yếu Chính phủ trong phòng, chống gián điệp mạng; bảo vệ thông tin thuộc bí mật nhà nước, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên không gian mạng; cụ thể:

Bộ Công an có trách nhiệm sau trừ trách nhiệm của Bộ Quốc phòng và Ban Cơ yếu Chính phủ theo quy định tại khoản 5, khoản 6 Điều 17 Luật An ninh mạng năm 2018: a) Kiểm tra an ninh mạng theo thẩm quyền đối với hệ thống thông tin quan trọng về an ninh quốc gia nhằm phát hiện, loại bỏ mã độc, phần cứng độc hại, khắc phục điểm yếu, lỗ hổng bảo mật; phát hiện, ngăn chặn, xử lý hoạt động xâm nhập bất hợp pháp; b) Kiểm tra an ninh mạng theo thẩm quyền đối với thiết bị, sản phẩm, dịch vụ thông tin liên lạc, thiết bị kỹ thuật số, thiết bị điện tử trước khi đưa vào sử dụng tại hệ thống thông tin quan trọng về an ninh quốc gia; c) Giám sát an ninh mạng theo thẩm quyền đối với hệ thống thông tin quan trọng về an ninh quốc gia nhằm phát hiện, xử lý hoạt động thu thập trái phép thông tin thuộc bí mật nhà nước; d) Phát hiện, xử lý các hành vi đăng tải, lưu trữ, trao đổi trái phép thông tin, tài liệu có nội dung thuộc bí mật

nhà nước trên không gian mạng; đ) Tham gia nghiên cứu, sản xuất sản phẩm lưu trữ, truyền đưa thông tin, tài liệu có nội dung thuộc bí mật nhà nước; sản phẩm mã hóa thông tin trên không gian mạng theo chức năng, nhiệm vụ được giao; e) Thanh tra, kiểm tra công tác bảo vệ bí mật nhà nước trên không gian mạng của cơ quan nhà nước và bảo vệ an ninh mạng của chủ quản hệ thống thông tin quan trọng về an ninh quốc gia; g) Tổ chức đào tạo, tập huấn nâng cao nhận thức và kiến thức về bảo vệ bí mật nhà nước trên không gian mạng, phòng, chống tấn công mạng, bảo vệ an ninh mạng đối với lực lượng bảo vệ an ninh mạng bố trí tại bộ, ngành, Ủy ban nhân dân cấp tỉnh, cơ quan, tổ chức quản lý trực tiếp hệ thống thông tin quan trọng về an ninh quốc gia (khoản 4 Điều 17).

Bộ Quốc phòng có trách nhiệm thực hiện các nội dung như trách nhiệm của Bộ Công an (trừ tổ chức đào tạo, tập huấn nâng cao nhận thức và kiến thức về bảo vệ bí mật nhà nước trên không gian mạng, phòng, chống tấn công mạng, bảo vệ an ninh mạng đối với lực lượng bảo vệ an ninh mạng bố trí tại bộ, ngành, Ủy ban nhân dân cấp tỉnh, cơ quan, tổ chức quản lý trực tiếp hệ thống thông tin quan trọng về an ninh quốc gia) đối với hệ thống thông tin quân sự (khoản 5 Điều 17).

Ban Cơ yếu Chính phủ có trách nhiệm tổ chức thực hiện các quy định của pháp luật trong việc

sử dụng mật mã để bảo vệ thông tin thuộc bí mật nhà nước được lưu trữ, trao đổi trên không gian mạng (khoản 6 Điều 17).

3. Về phòng, chống hành vi sử dụng không gian mạng, công nghệ thông tin, phương tiện điện tử để vi phạm pháp luật về an ninh quốc gia, trật tự, an toàn xã hội

Luật An ninh mạng năm 2018 quy định rõ ràng, cụ thể các hành vi sử dụng không gian mạng, công nghệ thông tin, phương tiện điện tử để vi phạm pháp luật về an ninh quốc gia, trật tự, an toàn xã hội bao gồm: a) Đăng tải, phát tán thông tin trên không gian mạng có nội dung quy định tại các khoản 1, 2, 3, 4 và 5 Điều 16 và hành vi quy định tại khoản 1 Điều 17 Luật An ninh mạng năm 2018; b) Chiếm đoạt tài sản; tổ chức đánh bạc, đánh bạc qua mạng internet; trộm cắp cước viễn thông quốc tế trên nền internet; vi phạm bản quyền và sở hữu trí tuệ trên không gian mạng; c) Giả mạo trang thông tin điện tử của cơ quan, tổ chức, cá nhân; làm giả, lưu hành, trộm cắp, mua bán, thu thập, trao đổi trái phép thông tin thẻ tín dụng, tài khoản ngân hàng của người khác; phát hành, cung cấp, sử dụng trái phép các phương tiện thanh toán; d) Tuyên truyền, quảng cáo, mua bán hàng hóa, dịch vụ thuộc danh mục cấm theo quy định của pháp luật; đ) Hướng dẫn người khác thực hiện hành vi vi phạm pháp luật; e) Hành vi khác

sử dụng không gian mạng, công nghệ thông tin, phương tiện điện tử để vi phạm pháp luật về an ninh quốc gia, trật tự, an toàn xã hội (khoản 1 Điều 18).

Cùng đó, Luật An ninh mạng năm 2018 quy định lực lượng chuyên trách bảo vệ an ninh mạng có trách nhiệm phòng, chống hành vi sử dụng không gian mạng, công nghệ thông tin, phương tiện điện tử để vi phạm pháp luật về an ninh quốc gia, trật tự, an toàn xã hội (khoản 2 Điều 18).

4. Về phòng, chống tấn công mạng

Các hành vi tấn công mạng và hành vi có liên quan đến tấn công mạng được quy định tại khoản 1 Điều 19 gồm: a) Phát tán chương trình tin học gây hại cho mạng viễn thông, mạng internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử; b) Gây cản trở, rối loạn, làm tê liệt, gián đoạn, ngưng trệ hoạt động, ngăn chặn trái phép việc truyền đưa dữ liệu của mạng viễn thông, mạng internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, phương tiện điện tử; c) Xâm nhập, làm tổn hại, chiếm đoạt dữ liệu được lưu trữ, truyền đưa qua mạng viễn thông, mạng internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử; d) Xâm nhập, tạo ra hoặc khai thác điểm yếu,

lỗ hổng bảo mật và dịch vụ hệ thống để chiếm đoạt thông tin, thu lợi bất chính; đ) Sản xuất, mua bán, trao đổi, tặng cho công cụ, thiết bị, phần mềm có tính năng tấn công mạng viễn thông, mạng internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử để sử dụng vào mục đích trái pháp luật; e) Hành vi khác gây ảnh hưởng đến hoạt động bình thường của mạng viễn thông, mạng internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử.

Đồng thời, Luật quy định trách nhiệm cho cơ quan chủ quản hệ thống thông tin trong việc áp dụng biện pháp kỹ thuật để phòng ngừa, ngăn chặn hành vi tấn công mạng và hành vi có liên quan đến tấn công mạng đối với hệ thống thông tin thuộc phạm vi quản lý (khoản 2 Điều 19). Trong trường hợp xảy ra tấn công mạng xâm phạm hoặc đe dọa xâm phạm chủ quyền, lợi ích, an ninh quốc gia, gây tổn hại nghiêm trọng trật tự, an toàn xã hội thì lực lượng chuyên trách bảo vệ an ninh mạng chủ trì, phối hợp với chủ quản hệ thống thông tin và tổ chức, cá nhân có liên quan áp dụng biện pháp xác định nguồn gốc tấn công mạng, thu thập chứng cứ; yêu cầu doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng internet, các dịch vụ gia tăng trên không gian mạng chặn lọc thông tin để ngăn chặn,

loại trừ hành vi tấn công mạng và cung cấp đầy đủ, kịp thời thông tin, tài liệu liên quan (khoản 3 Điều 19).

Cùng đó, khoản 4 Điều 19 Luật An ninh mạng năm 2018 quy định cụ thể trách nhiệm của Bộ Công an, Bộ Quốc phòng, Ban Cơ yếu Chính phủ trong công tác phòng, chống tấn công mạng. Theo đó, Bộ Công an chủ trì, phối hợp với bộ, ngành có liên quan thực hiện công tác phòng ngừa, phát hiện, xử lý hành vi quy định tại khoản 1 Điều 19 Luật An ninh mạng năm 2018 xâm phạm hoặc đe dọa xâm phạm chủ quyền, lợi ích, an ninh quốc gia, gây tổn hại nghiêm trọng trật tự, an toàn xã hội trên phạm vi cả nước, trừ trường hợp thuộc trách nhiệm của Bộ Quốc phòng, Ban Cơ yếu Chính phủ; Bộ Quốc phòng chủ trì, phối hợp với bộ, ngành có liên quan thực hiện công tác phòng ngừa, phát hiện, xử lý hành vi tấn công mạng và hành vi có liên quan đến tấn công mạng đối với hệ thống thông tin quân sự;

c) Ban Cơ yếu Chính phủ chủ trì, phối hợp với Bộ, ngành có liên quan thực hiện công tác phòng ngừa, phát hiện, xử lý hành vi tấn công mạng và hành vi có liên quan đến tấn công mạng đối với hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ.

5. Về phòng, chống khủng bố mạng

Khủng bố mạng là việc sử dụng không gian

mạng, công nghệ thông tin hoặc phương tiện điện tử để thực hiện hành vi khủng bố, tài trợ khủng bố.

Điều 20 Luật An ninh mạng năm 2018 quy định:

Cơ quan nhà nước có thẩm quyền có trách nhiệm áp dụng biện pháp theo quy định của Luật An ninh mạng năm 2018 và Điều 29 Luật An toàn thông tin mạng năm 2015, sửa đổi, bổ sung năm 2018 quy định về ngăn chặn hoạt động sử dụng mạng để khủng bố gồm: vô hiệu hóa nguồn internet sử dụng để thực hiện hành vi khủng bố; ngăn chặn việc thiết lập và mở rộng trao đổi thông tin về các tín hiệu, nhân tố, phương pháp và cách sử dụng internet để thực hiện hành vi khủng bố, về mục tiêu và hoạt động của các tổ chức khủng bố trên mạng; trao đổi kinh nghiệm và thực tiễn kiểm soát các nguồn internet, tìm và kiểm soát nội dung của trang tin điện tử có mục đích khủng bố.

Luật An ninh mạng năm 2018 quy định trách nhiệm của chủ quản hệ thống thông tin chủ động, thường xuyên rà soát, kiểm tra hệ thống thông tin thuộc phạm vi quản lý nhằm loại trừ nguy cơ khủng bố mạng. Khi phát hiện dấu hiệu, hành vi khủng bố mạng, cơ quan, tổ chức, cá nhân phải kịp thời báo cho lực lượng bảo vệ an ninh mạng. Cơ quan tiếp nhận tin báo có trách nhiệm tiếp nhận đầy đủ tin báo về khủng bố mạng và kịp thời thông báo cho lực lượng chuyên trách bảo vệ an ninh mạng.

Luật An ninh mạng năm 2018 cũng quy định cụ thể thẩm quyền, trách nhiệm của Bộ Công an, Bộ Quốc phòng, Ban Cơ yếu Chính phủ trong phòng, chống khủng bố mạng. Cụ thể như sau:

Bộ Công an chủ trì, phối hợp với bộ, ngành có liên quan triển khai công tác phòng, chống khủng bố mạng, áp dụng biện pháp vô hiệu hóa nguồn khủng bố mạng, xử lý khủng bố mạng, hạn chế đến mức thấp nhất hậu quả xảy ra đối với hệ thống thông tin, trừ trường hợp thuộc thẩm quyền của Bộ Quốc phòng, Ban Cơ yếu Chính phủ.

Bộ Quốc phòng chủ trì, phối hợp với bộ, ngành có liên quan triển khai công tác phòng, chống khủng bố mạng, áp dụng biện pháp xử lý khủng bố mạng xảy ra đối với hệ thống thông tin quân sự.

Ban Cơ yếu Chính phủ chủ trì, phối hợp với bộ, ngành có liên quan triển khai công tác phòng, chống khủng bố mạng, áp dụng biện pháp xử lý khủng bố mạng xảy ra đối với hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ.

6. Về phòng ngừa, xử lý tình huống nguy hiểm về an ninh mạng

Tình huống nguy hiểm về an ninh mạng theo quy định của Luật An ninh mạng năm 2018 tại khoản 1 Điều 21 bao gồm: a) Xuất hiện thông tin kích động trên không gian mạng có nguy cơ xảy ra bạo loạn, phá rối an ninh, khủng bố; b) Tấn công vào hệ thống thông tin quan trọng về an ninh

quốc gia; c) Tấn công nhiều hệ thống thông tin trên quy mô lớn, cường độ cao; d) Tấn công mạng nhằm phá hủy công trình quan trọng về an ninh quốc gia, mục tiêu quan trọng về an ninh quốc gia; đ) Tấn công mạng xâm phạm nghiêm trọng chủ quyền, lợi ích, an ninh quốc gia; gây tổn hại đặc biệt nghiêm trọng trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

Bên cạnh đó, để phòng ngừa tình huống nguy hiểm về an ninh mạng, Luật đã giao trách nhiệm đối với lực lượng chuyên trách bảo vệ an ninh mạng; doanh nghiệp viễn thông, internet, công nghệ thông tin, doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng internet, các dịch vụ gia tăng trên không gian mạng và cơ quan, tổ chức, cá nhân có liên quan (khoản 2 Điều 21). Cụ thể: (1) Đối với lực lượng chuyên trách bảo vệ an ninh mạng, phối hợp với chủ quản hệ thống thông tin quan trọng về an ninh quốc gia triển khai các giải pháp kỹ thuật, nghiệp vụ để phòng ngừa, phát hiện, xử lý tình huống nguy hiểm về an ninh mạng; (2) Doanh nghiệp viễn thông, internet, công nghệ thông tin, doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng internet, các dịch vụ gia tăng trên không gian mạng và cơ quan, tổ chức, cá nhân có liên quan có trách nhiệm phối hợp với Bộ Công an trong phòng ngừa, phát hiện, xử lý tình huống nguy hiểm về an ninh mạng.

Luật quy định về biện pháp xử lý tình huống nguy hiểm về an ninh mạng (khoản 3 Điều 21) và việc xử lý tình huống nguy hiểm về an ninh mạng (khoản 4 Điều 21). Theo đó, các biện pháp xử lý tình huống nguy hiểm về an ninh mạng gồm: a) Triển khai ngay phương án phòng ngừa, ứng phó khẩn cấp về an ninh mạng, ngăn chặn, loại trừ hoặc giảm nhẹ thiệt hại do tình huống nguy hiểm về an ninh mạng gây ra; b) Thông báo đến cơ quan, tổ chức, cá nhân có liên quan; c) Thu thập thông tin liên quan; theo dõi, giám sát liên tục đối với tình huống nguy hiểm về an ninh mạng; d) Phân tích, đánh giá thông tin, dự báo khả năng, phạm vi ảnh hưởng và mức độ thiệt hại do tình huống nguy hiểm về an ninh mạng gây ra; đ) Ngừng cung cấp thông tin mạng tại khu vực cụ thể hoặc ngắt cổng kết nối mạng quốc tế; e) Bố trí lực lượng, phương tiện ngăn chặn, loại bỏ tình huống nguy hiểm về an ninh mạng; g) Biện pháp khác theo quy định của Luật An ninh quốc gia. Việc xử lý tình huống nguy hiểm về an ninh mạng được thực hiện như sau: (1) Khi phát hiện tình huống nguy hiểm về an ninh mạng, cơ quan, tổ chức, cá nhân kịp thời thông báo cho lực lượng chuyên trách bảo vệ an ninh mạng và triển khai ngay phương án phòng ngừa, ứng phó khẩn cấp về an ninh mạng, ngăn chặn, loại trừ hoặc giảm nhẹ thiệt hại do tình huống nguy hiểm về an ninh mạng gây ra;

thông báo ngay đến cơ quan, tổ chức, cá nhân có liên quan; (2) Thủ tướng Chính phủ xem xét, quyết định hoặc ủy quyền cho Bộ trưởng Bộ Công an xem xét, quyết định, xử lý tình huống nguy hiểm về an ninh mạng trong phạm vi cả nước hoặc từng địa phương hoặc đối với một mục tiêu cụ thể. Thủ tướng Chính phủ xem xét, quyết định hoặc ủy quyền cho Bộ trưởng Bộ Quốc phòng xem xét, quyết định, xử lý tình huống nguy hiểm về an ninh mạng đối với hệ thống thông tin quân sự và hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ; (3) Lực lượng chuyên trách bảo vệ an ninh mạng chủ trì, phối hợp với cơ quan, tổ chức, cá nhân có liên quan áp dụng các biện pháp theo quy định tại khoản 3 Điều 21 Luật An ninh mạng năm 2018 để xử lý tình huống nguy hiểm về an ninh mạng; (4) Cơ quan, tổ chức, cá nhân có liên quan có trách nhiệm phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng thực hiện biện pháp nhằm ngăn chặn, xử lý tình huống nguy hiểm về an ninh mạng.

7. Về đấu tranh bảo vệ an ninh mạng

Đấu tranh bảo vệ an ninh mạng là hoạt động có tổ chức do lực lượng chuyên trách bảo vệ an ninh mạng thực hiện trên không gian mạng nhằm bảo vệ an ninh quốc gia và bảo đảm trật tự, an toàn xã hội.

Khoản 2 Điều 22 Luật An ninh mạng năm 2018 quy định nội dung đấu tranh bảo vệ an ninh mạng bao gồm:

(1) Tổ chức nắm tình hình có liên quan đến hoạt động bảo vệ an ninh quốc gia;

(2) Phòng, chống tấn công và bảo vệ hoạt động ổn định của hệ thống thông tin quan trọng về an ninh quốc gia;

(3) Làm tê liệt hoặc hạn chế hoạt động sử dụng không gian mạng nhằm gây phương hại an ninh quốc gia hoặc gây tổn hại đặc biệt nghiêm trọng trật tự, an toàn xã hội;

(4) Chủ động tấn công vô hiệu hóa mục tiêu trên không gian mạng nhằm bảo vệ an ninh quốc gia và bảo đảm trật tự, an toàn xã hội.

Luật An ninh mạng năm 2018 quy định Bộ Công an là cơ quan được giao chủ trì, phối hợp với bộ, ngành có liên quan thực hiện đấu tranh bảo vệ an ninh mạng.

IV. HOẠT ĐỘNG BẢO VỆ AN NINH MẠNG

Luật An ninh mạng năm 2018 quy định một chương (Chương IV) quy định về hoạt động bảo vệ an ninh mạng. Chương này tập trung quy định về triển khai hoạt động bảo vệ an ninh mạng một cách đồng bộ, thống nhất từ trung ương tới địa phương, trọng tâm là các cơ quan nhà nước và tổ chức chính trị, quy định rõ các nội dung triển khai,

hoạt động kiểm tra an ninh mạng đối với hệ thống thông tin của các cơ quan, tổ chức này. Cơ sở hạ tầng không gian mạng quốc gia, cổng kết nối mạng quốc tế cũng là một trong những đối tượng được bảo vệ trọng điểm. Với các quy định chặt chẽ, sự tham gia đồng bộ của cơ quan nhà nước, doanh nghiệp và tổ chức, cá nhân, việc sử dụng thông tin để vu khống, làm nhục, xâm phạm danh dự, nhân phẩm, uy tín của người khác sẽ được xử lý nghiêm minh. Các hoạt động nghiên cứu, phát triển an ninh mạng, phát triển công nghệ, sản phẩm, dịch vụ, ứng dụng nhằm bảo vệ an ninh mạng, nâng cao năng lực tự chủ về an ninh mạng và bảo vệ trẻ em trên không gian mạng cũng được quy định chi tiết trong Chương này.

1. Về triển khai hoạt động bảo vệ an ninh mạng trong cơ quan nhà nước, tổ chức chính trị ở trung ương và địa phương

Luật An ninh mạng năm 2018 quy định nội dung triển khai hoạt động bảo vệ an ninh mạng tại khoản 1 Điều 23 bao gồm: a) Xây dựng, hoàn thiện quy định, quy chế sử dụng mạng máy tính nội bộ, mạng máy tính có kết nối mạng internet; phương án bảo đảm an ninh mạng đối với hệ thống thông tin; phương án ứng phó, khắc phục sự cố an ninh mạng; b) Ứng dụng, triển khai phương án, biện pháp, công nghệ bảo vệ an ninh mạng đối với hệ thống thông tin và thông tin,

tài liệu được lưu trữ, soạn thảo, truyền đưa trên hệ thống thông tin thuộc phạm vi quản lý; c) Tổ chức bồi dưỡng kiến thức về an ninh mạng cho cán bộ, công chức, viên chức, người lao động; nâng cao năng lực bảo vệ an ninh mạng cho lực lượng bảo vệ an ninh mạng; d) Bảo vệ an ninh mạng trong hoạt động cung cấp dịch vụ công trên không gian mạng, cung cấp, trao đổi, thu thập thông tin với cơ quan, tổ chức, cá nhân, chia sẻ thông tin trong nội bộ và với cơ quan khác hoặc trong hoạt động khác theo quy định của Chính phủ; đ) Đầu tư, xây dựng hạ tầng cơ sở vật chất phù hợp với điều kiện bảo đảm triển khai hoạt động bảo vệ an ninh mạng đối với hệ thống thông tin; e) Kiểm tra an ninh mạng đối với hệ thống thông tin; phòng, chống hành vi vi phạm pháp luật về an ninh mạng; ứng phó, khắc phục sự cố an ninh mạng (khoản 1 Điều 23).

Bên cạnh đó, Luật quy định người đứng đầu cơ quan, tổ chức có trách nhiệm triển khai hoạt động bảo vệ an ninh mạng thuộc quyền quản lý (khoản 2 Điều 23).

2. Kiểm tra an ninh mạng đối với hệ thống thông tin của cơ quan, tổ chức không thuộc Danh mục hệ thống thông tin quan trọng về an ninh quốc gia

Việc kiểm tra an ninh mạng đối với hệ thống thông tin của cơ quan, tổ chức không thuộc

Danh mục hệ thống thông tin quan trọng về an ninh quốc gia quy định tại khoản 1 Điều 24 trong các trường hợp sau đây: (1) Khi có hành vi vi phạm pháp luật về an ninh mạng xâm phạm an ninh quốc gia hoặc gây tổn hại nghiêm trọng trật tự, an toàn xã hội; (2) Khi có đề nghị của chủ quản hệ thống thông tin.

Về đối tượng kiểm tra an ninh mạng quy định tại khoản 2 Điều 24 bao gồm: (1) Hệ thống phần cứng, phần mềm, thiết bị số được sử dụng trong hệ thống thông tin; (2) Thông tin được lưu trữ, xử lý, truyền đưa trong hệ thống thông tin; (3) Biện pháp bảo vệ bí mật nhà nước và phòng, chống lộ, mất bí mật nhà nước qua các kênh kỹ thuật.

Luật An ninh mạng năm 2018 giao trách nhiệm cho chủ quản hệ thống thông tin (khoản 3 Điều 24), lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an (khoản 4 Điều 24) và các quy định trước thời điểm kiểm tra và sau khi kết thúc kiểm tra (khoản 5 Điều 24). Kết quả kiểm tra an ninh mạng được bảo mật theo quy định của pháp luật (khoản 6 Điều 24). Cụ thể:

- Chủ quản hệ thống thông tin có trách nhiệm thông báo cho lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an khi phát hiện hành vi vi phạm pháp luật về an ninh mạng trên hệ thống thông tin thuộc phạm vi quản lý.

- Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an tiến hành kiểm tra an ninh

mạng đối với hệ thống thông tin của cơ quan, tổ chức khi có hành vi vi phạm pháp luật về an ninh mạng xâm phạm an ninh quốc gia hoặc gây tổn hại nghiêm trọng trật tự, an toàn xã hội; khi có đề nghị của chủ quản hệ thống thông tin.

- Trước thời điểm tiến hành kiểm tra, lực lượng chuyên trách bảo vệ an ninh mạng thông báo bằng văn bản cho chủ quản hệ thống thông tin ít nhất 12 giờ. Trong thời hạn 30 ngày kể từ ngày kết thúc kiểm tra, lực lượng chuyên trách bảo vệ an ninh mạng thông báo kết quả kiểm tra và đưa ra yêu cầu đối với chủ quản hệ thống thông tin trong trường hợp phát hiện điểm yếu, lỗ hổng bảo mật; hướng dẫn hoặc tham gia khắc phục khi có đề nghị của chủ quản hệ thống thông tin.

Đồng thời, Luật An ninh mạng năm 2018 giao Chính phủ quy định trình tự, thủ tục kiểm tra an ninh mạng đối với hệ thống thông tin của cơ quan, tổ chức không thuộc Danh mục hệ thống thông tin quan trọng về an ninh quốc gia.

3. Về bảo vệ an ninh mạng đối với cơ sở hạ tầng không gian mạng quốc gia, cổng kết nối mạng quốc tế

Khoản 1 Điều 25 Luật An ninh mạng năm 2018 quy định bảo vệ an ninh mạng đối với cơ sở hạ tầng không gian mạng quốc gia, cổng kết nối mạng quốc tế phải bảo đảm kết hợp chặt chẽ giữa yêu cầu bảo vệ an ninh mạng với yêu cầu xây

dựng, phát triển kinh tế - xã hội; khuyến khích cổng kết nối quốc tế đặt trên lãnh thổ Việt Nam; khuyến khích tổ chức, cá nhân tham gia đầu tư xây dựng cơ sở hạ tầng không gian mạng quốc gia.

Đồng thời, tại khoản 2 Điều 25 Luật An ninh mạng năm 2018 quy định trách nhiệm của cơ quan, tổ chức, cá nhân quản lý, khai thác cơ sở hạ tầng không gian mạng quốc gia, cổng kết nối mạng quốc tế; gồm các nội dung sau:

(1) Bảo vệ an ninh mạng thuộc quyền quản lý; chịu sự quản lý, thanh tra, kiểm tra và thực hiện các yêu cầu về bảo vệ an ninh mạng của cơ quan nhà nước có thẩm quyền;

(2) Tạo điều kiện; thực hiện các biện pháp kỹ thuật, nghiệp vụ cần thiết để cơ quan nhà nước có thẩm quyền thực hiện nhiệm vụ bảo vệ an ninh mạng khi có đề nghị.

4. Về bảo đảm an ninh thông tin trên không gian mạng

Để bảo đảm an ninh thông tin trên không gian mạng, Luật An ninh mạng năm 2018 quy định đối với trang thông tin điện tử, cổng thông tin điện tử hoặc chuyên trang trên mạng xã hội của cơ quan, tổ chức, cá nhân không được cung cấp, đăng tải, truyền đưa thông tin trên không gian mạng có nội dung tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam; kích động gây bạo loạn, phá rối an ninh, gây rối trật tự

công cộng; làm nhục, vu khống; xâm phạm trật tự quản lý kinh tế quy định tại các khoản: 1, 2, 3, 4 và 5 Điều 16 Luật An ninh mạng năm 2018 và thông tin khác có nội dung xâm phạm an ninh quốc gia (khoản 1 Điều 26).

Để quản lý chặt chẽ, bảo vệ nghiêm ngặt dữ liệu của nước ta trên không gian mạng, Luật An ninh mạng năm 2018 quy định đối với doanh nghiệp trong nước và ngoài nước cung cấp dịch vụ trên mạng viễn thông, mạng internet, các dịch vụ gia tăng trên không gian mạng tại Việt Nam có trách nhiệm: (1) Xác thực thông tin khi người dùng đăng ký tài khoản số; bảo mật thông tin, tài khoản của người dùng; cung cấp thông tin người dùng cho lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an khi có yêu cầu bằng văn bản để phục vụ điều tra, xử lý hành vi vi phạm pháp luật về an ninh mạng; (2) Ngăn chặn việc chia sẻ thông tin, xóa bỏ thông tin có nội dung tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam; kích động gây bạo loạn, phá rối an ninh, gây rối trật tự công cộng; làm nhục, vu khống; xâm phạm trật tự quản lý kinh tế quy định tại các khoản 1, 2, 3, 4 và 5 Điều 16 Luật An ninh mạng năm 2018 trên dịch vụ hoặc hệ thống thông tin do cơ quan, tổ chức trực tiếp quản lý chậm nhất là 24 giờ kể từ thời điểm có yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an hoặc cơ quan có

thẩm quyền của Bộ Thông tin và Truyền thông và lưu nhật ký hệ thống để phục vụ điều tra, xử lý hành vi vi phạm pháp luật về an ninh mạng trong thời gian theo quy định của Chính phủ; (3) Không cung cấp hoặc ngừng cung cấp dịch vụ trên mạng viễn thông, mạng internet, các dịch vụ gia tăng cho tổ chức, cá nhân đăng tải trên không gian mạng thông tin có nội dung tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam; kích động gây bạo loạn, phá rối an ninh, gây rối trật tự công cộng; làm nhục, vu khống; xâm phạm trật tự quản lý kinh tế quy định tại các khoản 1, 2, 3, 4 và 5 Điều 16 Luật An ninh mạng năm 2018 khi có yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an hoặc cơ quan có thẩm quyền của Bộ Thông tin và Truyền thông (khoản 2 Điều 26).

Đối với doanh nghiệp trong nước và ngoài nước cung cấp dịch vụ trên mạng viễn thông, mạng internet, các dịch vụ gia tăng trên không gian mạng tại Việt Nam có hoạt động thu thập, khai thác, phân tích, xử lý dữ liệu về thông tin cá nhân, dữ liệu về mối quan hệ của người sử dụng dịch vụ, dữ liệu do người sử dụng dịch vụ tại Việt Nam tạo ra phải lưu trữ dữ liệu này tại Việt Nam trong thời gian theo quy định của Chính phủ; doanh nghiệp ngoài nước cung cấp dịch vụ trên mạng viễn thông, mạng internet, các dịch vụ gia tăng trên không gian mạng tại Việt Nam có hoạt

động thu thập, khai thác, phân tích, xử lý dữ liệu về thông tin cá nhân, dữ liệu về mối quan hệ của người sử dụng dịch vụ, dữ liệu do người sử dụng dịch vụ tại Việt Nam tạo ra phải đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam (khoản 3 Điều 26). Cùng đó, Luật An ninh mạng năm 2018 giao Chính phủ quy định chi tiết khoản 3 Điều 26 Luật An ninh mạng năm 2018.

Như vậy, doanh nghiệp trong nước và ngoài nước khi cung cấp dịch vụ trên mạng viễn thông, mạng internet và các dịch vụ gia tăng trên không gian mạng tại Việt Nam có trách nhiệm xác thực thông tin khi người dùng đăng ký tài khoản số; bảo mật thông tin, tài khoản của người dùng và chỉ trong trường hợp phục vụ điều tra, xử lý hành vi vi phạm pháp luật về an ninh mạng, lực lượng chuyên trách bảo vệ an ninh mạng mới được quyền yêu cầu cung cấp thông tin người dùng. Mặt khác, thông tin cá nhân vi phạm pháp luật là một trong những loại dữ liệu quan trọng phục vụ điều tra, xử lý hành vi vi phạm pháp luật. Lực lượng bảo vệ pháp luật chỉ được phép yêu cầu cung cấp thông tin trong trường hợp phục vụ xử lý vi phạm pháp luật. Các quy định trong Bộ luật Tố tụng hình sự năm 2015 và các văn bản có liên quan đã quy định rõ về việc quản lý, sử dụng thông tin được cung cấp để phục vụ điều tra, xử lý các hành vi vi phạm pháp luật. Trước các hoạt động vi phạm pháp luật trên không gian mạng đang diễn ra nghiêm trọng,

phức tạp, yêu cầu bảo đảm cơ sở, điều kiện để điều tra, xử lý nhanh chóng, hiệu quả của lực lượng bảo vệ pháp luật là cần thiết, cấp bách, trong đó có trách nhiệm của các doanh nghiệp cung cấp dịch vụ trong và ngoài nước.

Việc quy định các doanh nghiệp nước ngoài cung cấp dịch vụ trên không gian mạng phải cung cấp thông tin người dùng cho lực lượng chuyên trách bảo vệ an ninh mạng là phù hợp với pháp luật Việt Nam cũng như phù hợp với thông lệ quốc tế khi trong bối cảnh hiện nay, tất cả các quốc gia trên thế giới đều coi an ninh quốc gia là điều kiện tiên quyết hàng đầu, do đó, các doanh nghiệp cung cấp dịch vụ trên không gian mạng đã và đang phải phối hợp với các cơ quan chức năng của các quốc gia trên thế giới trong bảo vệ an ninh quốc gia, phòng chống tội phạm. Khoản 2 Điều 26 Luật An ninh mạng năm 2018 quy định rõ các trường hợp phải cung cấp thông tin cho lực lượng chuyên trách bảo vệ an ninh mạng. Đây là hai điều kiện đồng thời, tức là khi có hành vi vi phạm pháp luật về an ninh mạng xảy ra thì lực lượng chuyên trách bảo vệ an ninh mạng sẽ có văn bản yêu cầu các doanh nghiệp nêu trên cung cấp thông tin về hành vi vi phạm pháp luật đó. Cần đặc biệt lưu ý rằng, những thông tin cung cấp là thông tin liên quan tới hành vi vi phạm pháp luật.

Đối với quy định tại khoản 3 Điều 26 Luật An ninh mạng năm 2018 về lưu trữ dữ liệu tại

Việt Nam: doanh nghiệp phải chịu điều chỉnh theo quy định này là những doanh nghiệp trong và ngoài nước cung cấp dịch vụ trên mạng viễn thông, mạng internet và các dịch vụ gia tăng trên không gian mạng tại Việt Nam có hoạt động thu thập, khai thác, phân tích, xử lý dữ liệu người dùng Việt Nam. Quy định này không áp dụng đối với toàn bộ các doanh nghiệp mà là những doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng internet và các dịch vụ gia tăng trên không gian mạng tại Việt Nam, nhưng phải kèm theo điều kiện có hoạt động thu thập, khai thác, phân tích, xử lý dữ liệu người dùng tại Việt Nam. Quy định này là phù hợp với yêu cầu bảo vệ an ninh mạng hiện nay; đồng thời, Luật An ninh mạng năm 2018 đã quy định cụ thể 03 loại dữ liệu cần lưu trữ (thông tin cá nhân người sử dụng dịch vụ; dữ liệu về mối quan hệ của người sử dụng dịch vụ; dữ liệu do người sử dụng dịch vụ tại Việt Nam tạo ra). Như vậy, không phải toàn bộ các dữ liệu được truyền đưa trên không gian mạng phải lưu trữ tại Việt Nam; do đó, quy định này không làm ảnh hưởng tới lưu thông dữ liệu số, cản trở hoạt động của doanh nghiệp.

5. Về nghiên cứu, phát triển an ninh mạng

Luật An ninh mạng năm 2018 quy định, nội dung nghiên cứu, phát triển an ninh mạng bao gồm: a) Xây dựng hệ thống phần mềm, trang

thiết bị bảo vệ an ninh mạng; b) Phương pháp thẩm định phần mềm, trang thiết bị bảo vệ an ninh mạng đạt chuẩn và hạn chế tồn tại điểm yếu, lỗ hổng bảo mật, phần mềm độc hại; c) Phương pháp kiểm tra phần cứng, phần mềm được cung cấp thực hiện đúng chức năng; d) Phương pháp bảo vệ bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư; khả năng bảo mật khi truyền đưa thông tin trên không gian mạng; đ) Xác định nguồn gốc của thông tin được truyền đưa trên không gian mạng; e) Giải quyết nguy cơ đe dọa an ninh mạng; g) Xây dựng thao trường mạng, môi trường thử nghiệm an ninh mạng; h) Sáng kiến kỹ thuật nâng cao nhận thức, kỹ năng về an ninh mạng; i) Dự báo an ninh mạng; k) Nghiên cứu thực tiễn, phát triển lý luận an ninh mạng (khoản 1 Điều 27). Bên cạnh đó, Luật An ninh mạng năm 2018 quy định các cơ quan, tổ chức, cá nhân có liên quan đều có quyền nghiên cứu, phát triển an ninh mạng mà không giới hạn.

6. Về nâng cao năng lực tự chủ về an ninh mạng

Để nâng cao năng lực tự chủ về an ninh mạng, Luật An ninh mạng năm 2018 đã thể chế hóa chính sách của Nhà nước về phát triển nền công nghệ thông tin vững mạnh, tự chủ bằng việc ban hành một điều trong Luật An ninh mạng

năm 2018 (Điều 28) quy định về nâng cao năng lực tự chủ về an ninh mạng. Luật An ninh mạng năm 2018 quy định Nhà nước khuyến khích, tạo điều kiện để cơ quan, tổ chức, cá nhân nâng cao năng lực tự chủ về an ninh mạng và nâng cao khả năng sản xuất, kiểm tra, đánh giá, kiểm định thiết bị số, dịch vụ mạng, ứng dụng mạng (khoản 1 Điều 28). Đồng thời, Luật An ninh mạng năm 2018 quy định Chính phủ thực hiện các biện pháp nâng cao năng lực tự chủ về an ninh mạng cho cơ quan, tổ chức, cá nhân: a) Thúc đẩy chuyển giao, nghiên cứu, làm chủ và phát triển công nghệ, sản phẩm, dịch vụ, ứng dụng để bảo vệ an ninh mạng; b) Thúc đẩy ứng dụng công nghệ mới, công nghệ tiên tiến liên quan đến an ninh mạng; c) Tổ chức đào tạo, phát triển và sử dụng nhân lực an ninh mạng; d) Tăng cường môi trường kinh doanh, cải thiện điều kiện cạnh tranh hỗ trợ doanh nghiệp nghiên cứu, sản xuất sản phẩm, dịch vụ, ứng dụng để bảo vệ an ninh mạng (khoản 2 Điều 28).

7. Bảo vệ trẻ em trên không gian mạng

Theo quy định của Điều 1 Luật Trẻ em năm 2016, sửa đổi, bổ sung năm 2018, trẻ em là người dưới 16 tuổi; bảo vệ trẻ em là việc thực hiện các biện pháp phù hợp để bảo đảm trẻ em được sống an toàn, lành mạnh; phòng ngừa, ngăn chặn và

xử lý các hành vi xâm hại trẻ em; trợ giúp trẻ em có hoàn cảnh đặc biệt.

Theo đó, để đáp ứng yêu cầu thực tiễn, đồng thời thể hiện chính sách bảo vệ trẻ em của Nhà nước ta, Luật An ninh mạng năm 2018 quy định, trẻ em có quyền được bảo vệ, tiếp cận thông tin, tham gia hoạt động xã hội, vui chơi, giải trí, giữ bí mật cá nhân, đời sống riêng tư và các quyền khác khi tham gia trên không gian mạng (khoản 1 Điều 29). Đây là quy định rất tiến bộ trong Luật An ninh mạng năm 2018. Bên cạnh đó, Luật quy định cụ thể trách nhiệm của chủ quản hệ thống thông tin, doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng internet, các dịch vụ gia tăng trên không gian mạng (khoản 2 Điều 29); cơ quan, tổ chức cá nhân tham gia hoạt động không gian mạng (khoản 3 Điều 29); cơ quan, tổ chức, cha mẹ, giáo viên, người chăm sóc trẻ em và cá nhân khác liên quan (khoản 4 Điều 29); lực lượng chuyên trách bảo vệ an ninh mạng và các cơ quan chức năng (khoản 5 Điều 29). Cụ thể:

Đối với chủ quản hệ thống thông tin, doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng internet và các dịch vụ gia tăng trên không gian mạng, có trách nhiệm kiểm soát nội dung thông tin trên hệ thống thông tin hoặc trên dịch vụ do doanh nghiệp cung cấp để không gây nguy hại cho trẻ em, xâm phạm đến trẻ em, quyền trẻ em; ngăn chặn việc chia sẻ và xóa bỏ thông tin có

nội dung gây nguy hại cho trẻ em, xâm phạm đến trẻ em, quyền trẻ em; kịp thời thông báo, phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an để xử lý.

Đối với cơ quan, tổ chức, cá nhân tham gia hoạt động trên không gian mạng có trách nhiệm phối hợp với cơ quan quản lý nhà nước có thẩm quyền trong bảo đảm quyền của trẻ em trên không gian mạng, ngăn chặn thông tin mạng gây nguy hại cho trẻ em theo quy định của Luật An ninh mạng năm 2018 và pháp luật về trẻ em.

Đối với cơ quan, tổ chức, cha, mẹ, giáo viên, người chăm sóc trẻ em và cá nhân khác liên quan có trách nhiệm bảo đảm quyền của trẻ em, bảo vệ trẻ em khi tham gia không gian mạng theo quy định của pháp luật về trẻ em.

Đối với lực lượng chuyên trách bảo vệ an ninh mạng và các cơ quan chức năng có trách nhiệm áp dụng biện pháp để phòng ngừa, phát hiện, ngăn chặn, xử lý nghiêm hành vi sử dụng không gian mạng gây nguy hại cho trẻ em, xâm phạm đến trẻ em, quyền trẻ em.

V. VỀ BẢO ĐẢM HOẠT ĐỘNG BẢO VỆ AN NINH MẠNG

Nguồn nhân lực bảo vệ an ninh mạng là một trong những yếu tố quyết định sự thành bại của công tác bảo vệ an ninh mạng. Luật An ninh mạng

năm 2018 quy định đầy đủ các nội dung bảo đảm triển khai hoạt động bảo vệ an ninh mạng, xác định lực lượng chuyên trách bảo vệ an ninh mạng, ưu tiên đào tạo nguồn nhân lực an ninh mạng chất lượng cao, chú trọng giáo dục, bồi dưỡng, phổ biến kiến thức về an ninh mạng tại Chương V.

1. Về lực lượng bảo vệ an ninh mạng

Điều 30 Luật An ninh mạng năm 2018 quy định lực lượng bảo vệ an ninh mạng bao gồm lực lượng chuyên trách bảo vệ an ninh mạng, lực lượng bảo vệ an ninh mạng và tổ chức, cá nhân được huy động tham gia bảo vệ an ninh mạng. Theo Điều 30 Luật An ninh mạng năm 2018, thì chỉ Bộ Công an, Bộ Quốc phòng mới được bố trí lực lượng chuyên trách bảo vệ an ninh mạng được bố trí tại Bộ Công an, Bộ Quốc phòng còn lực lượng bảo vệ an ninh mạng được bố trí tại bộ, ngành, Ủy ban nhân dân cấp tỉnh, cơ quan, tổ chức quản lý trực tiếp hệ thống thông tin quan trọng về an ninh quốc gia. Ngoài ra, trong trường hợp cần thiết thì tổ chức, cá nhân có thể được huy động tham gia bảo vệ an ninh mạng.

2. Về bảo đảm nguồn nhân lực bảo vệ an ninh mạng

Điều 31 Luật An ninh mạng năm 2018 quy định công dân Việt Nam có kiến thức về an ninh mạng, an toàn thông tin mạng, công nghệ thông

tin là nguồn lực cơ bản, chủ yếu bảo vệ an ninh mạng; Nhà nước có chương trình, kế hoạch xây dựng, phát triển nguồn nhân lực bảo vệ an ninh mạng. Đồng thời, tại khoản 3 Điều 31 quy định cơ quan nhà nước có thẩm quyền quyết định huy động nhân lực bảo vệ an ninh mạng khi xảy ra tình huống nguy hiểm về an ninh mạng, khủng bố mạng, tấn công mạng, sự cố an ninh mạng hoặc nguy cơ đe dọa an ninh mạng. Cùng với đó, quy định thẩm quyền, trách nhiệm, trình tự, thủ tục huy động nhân lực bảo vệ an ninh mạng được thực hiện theo quy định của Luật An ninh quốc gia, Luật Quốc phòng, Luật Công an nhân dân và quy định khác của pháp luật có liên quan.

3. Về việc tuyển chọn, đào tạo, phát triển lực lượng bảo vệ an ninh mạng

Điều 32 Luật An ninh mạng năm 2018 quy định công dân Việt Nam có đủ tiêu chuẩn về phẩm chất đạo đức, sức khỏe, trình độ, kiến thức về an ninh mạng, an toàn thông tin mạng, công nghệ thông tin, có nguyện vọng thì có thể được tuyển chọn vào lực lượng bảo vệ an ninh mạng; ưu tiên đào tạo, phát triển lực lượng bảo vệ an ninh mạng có chất lượng cao; ưu tiên phát triển cơ sở đào tạo an ninh mạng đạt tiêu chuẩn quốc tế; khuyến khích liên kết, tạo cơ hội hợp tác về an ninh mạng giữa khu vực nhà nước và khu vực tư nhân, trong nước và ngoài nước.

4. Về giáo dục, bồi dưỡng kiến thức, nghiệp vụ an ninh mạng

Luật An ninh mạng năm 2018 quy định cụ thể nội dung giáo dục, bồi dưỡng kiến thức an ninh mạng được đưa vào môn học giáo dục quốc phòng và an ninh trong nhà trường và chương trình bồi dưỡng kiến thức quốc phòng và an ninh theo quy định của Luật Giáo dục quốc phòng và an ninh.

Tại Điều 33 Luật An ninh mạng năm 2018 quy định Bộ Công an là cơ quan chủ trì, phối hợp với bộ, ngành có liên quan tổ chức bồi dưỡng nghiệp vụ an ninh mạng cho lực lượng bảo vệ an ninh mạng và công chức, viên chức, người lao động tham gia bảo vệ an ninh mạng. Đồng thời, để bảo đảm phù hợp chức năng, nhiệm vụ của Bộ Quốc phòng, Ban Cơ yếu Chính phủ, Luật An ninh mạng năm 2018 quy định Bộ Quốc phòng, Ban Cơ yếu Chính phủ tổ chức bồi dưỡng nghiệp vụ an ninh mạng cho lực lượng thuộc phạm vi quản lý.

5. Về phổ biến kiến thức về an ninh mạng

Điều 34 Luật An ninh mạng năm 2018 quy định Nhà nước có chính sách phổ biến kiến thức về an ninh mạng trong phạm vi cả nước, khuyến khích cơ quan nhà nước phối hợp với tổ chức tư nhân, cá nhân thực hiện chương trình giáo dục

và nâng cao nhận thức về an ninh mạng. Đối với bộ, ngành, cơ quan, tổ chức có trách nhiệm xây dựng và triển khai hoạt động phổ biến kiến thức về an ninh mạng cho cán bộ, công chức, viên chức, người lao động trong cơ quan, tổ chức. Đối với Ủy ban nhân dân cấp tỉnh có trách nhiệm xây dựng và triển khai hoạt động phổ biến kiến thức, nâng cao nhận thức về an ninh mạng cho cơ quan, tổ chức, cá nhân của địa phương.

6. Về kinh phí bảo vệ an ninh mạng

Điều 35 Luật An ninh mạng năm 2018 quy định kinh phí bảo vệ an ninh mạng của cơ quan nhà nước, tổ chức chính trị do ngân sách nhà nước bảo đảm, được sử dụng trong dự toán ngân sách nhà nước hằng năm. Việc quản lý, sử dụng kinh phí từ ngân sách nhà nước thực hiện theo quy định của pháp luật về ngân sách nhà nước. Đối với kinh phí bảo vệ an ninh mạng cho hệ thống thông tin của cơ quan, tổ chức còn lại do cơ quan, tổ chức tự bảo đảm.

VI. VỀ TRÁCH NHIỆM CỦA CƠ QUAN, TỔ CHỨC, CÁ NHÂN

Trách nhiệm của cơ quan, tổ chức, cá nhân được quy định tại Chương VI Luật An ninh mạng năm 2018, theo chức năng, nhiệm vụ được giao Bộ Công an, Bộ Quốc phòng, Bộ Thông tin và

Truyền thông, Ban Cơ yếu Chính phủ, các bộ, ngành, Ủy ban nhân dân cấp tỉnh, doanh nghiệp cung cấp dịch vụ trên không gian mạng và cơ quan, tổ chức, cá nhân sử dụng không gian mạng thực hiện đồng bộ các biện pháp được phân công để hướng tới một không gian mạng ít nguy cơ, hạn chế tối đa các hành vi vi phạm pháp luật trên không gian mạng.

1. Về trách nhiệm của Bộ Công an

Theo quy định tại Điều 36 Luật An ninh mạng năm 2018, Bộ Công an chịu trách nhiệm trước Chính phủ thực hiện quản lý nhà nước về an ninh mạng và có nhiệm vụ, quyền hạn sau đây, trừ nội dung thuộc trách nhiệm của Bộ Quốc phòng và Ban Cơ yếu Chính phủ: (1) Ban hành hoặc trình cơ quan nhà nước có thẩm quyền ban hành và hướng dẫn thi hành văn bản quy phạm pháp luật về an ninh mạng; (2) Xây dựng, đề xuất chiến lược, chủ trương, chính sách, kế hoạch và phương án bảo vệ an ninh mạng; (3) Phòng ngừa, đấu tranh với hoạt động sử dụng không gian mạng xâm phạm chủ quyền, lợi ích, an ninh quốc gia, trật tự, an toàn xã hội và phòng, chống tội phạm mạng; (4) Bảo đảm an ninh thông tin trên không gian mạng; xây dựng cơ chế xác thực thông tin đăng ký tài khoản số; cảnh báo, chia sẻ thông tin an ninh mạng, nguy cơ đe dọa an ninh mạng; (5) Tham mưu, đề xuất

Chính phủ, Thủ tướng Chính phủ xem xét, quyết định việc phân công, phối hợp thực hiện các biện pháp bảo vệ an ninh mạng, phòng ngừa, xử lý hành vi xâm phạm an ninh mạng trong trường hợp nội dung quản lý nhà nước liên quan đến phạm vi quản lý của nhiều bộ, ngành; (6) Tổ chức diễn tập phòng, chống tấn công mạng; diễn tập ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia; (7) Kiểm tra, thanh tra, giải quyết khiếu nại, tố cáo và xử lý vi phạm pháp luật về an ninh mạng.

2. Về trách nhiệm của Bộ Quốc phòng

Luật An ninh mạng năm 2018 quy định Bộ Quốc phòng chịu trách nhiệm trước Chính phủ thực hiện quản lý nhà nước về an ninh mạng trong phạm vi quản lý và có nhiệm vụ, quyền hạn tương tự như của Bộ Công an về nội dung công tác trong thực hiện quản lý nhà nước về an ninh mạng trong phạm vi thẩm quyền quản lý. Theo quy định của Điều 37 Luật An ninh mạng năm 2018, Bộ Quốc phòng chịu trách nhiệm trước Chính phủ thực hiện quản lý nhà nước về an ninh mạng trong phạm vi quản lý và có nhiệm vụ, quyền hạn sau đây:

1. Ban hành hoặc trình cơ quan nhà nước có thẩm quyền ban hành và hướng dẫn thi hành văn bản quy phạm pháp luật về an ninh mạng trong phạm vi quản lý;

2. Xây dựng, đề xuất chiến lược, chủ trương, chính sách, kế hoạch và phương án bảo vệ an ninh mạng trong phạm vi quản lý;

3. Phòng ngừa, đấu tranh với các hoạt động sử dụng không gian mạng xâm phạm an ninh quốc gia trong phạm vi quản lý;

4. Phối hợp với Bộ Công an tổ chức diễn tập phòng, chống tấn công mạng; diễn tập ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia; triển khai thực hiện công tác bảo vệ an ninh mạng;

5. Kiểm tra, thanh tra, giải quyết khiếu nại, tố cáo và xử lý vi phạm pháp luật về an ninh mạng trong phạm vi quản lý.

Để bảo đảm hiệu quả trong công tác bảo đảm an ninh mạng, Luật An ninh mạng năm 2018 quy định về quan hệ phối hợp giữa Bộ Công an và Bộ Quốc phòng tại khoản 4 Điều 37. Theo đó, Bộ Quốc phòng phối hợp với Bộ Công an - cơ quan chịu trách nhiệm trước Chính phủ thực hiện quản lý nhà nước về an ninh mạng trong tổ chức diễn tập phòng, chống tấn công mạng, diễn tập ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia, triển khai thực hiện công tác bảo vệ an ninh mạng.

3. Về trách nhiệm của Bộ Thông tin và Truyền thông

Điều 38 Luật An ninh mạng năm 2018 quy

định Bộ Thông tin và Truyền thông có trách nhiệm: (1) Phối hợp với Bộ Công an, Bộ Quốc phòng trong bảo vệ an ninh mạng; (2) Phối hợp với các cơ quan liên quan tổ chức tuyên truyền, phản bác thông tin có nội dung chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam quy định tại khoản 1 Điều 16 Luật An ninh mạng năm 2018; (3) Yêu cầu doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng internet, các dịch vụ gia tăng trên không gian mạng, chủ quản hệ thống thông tin loại bỏ thông tin có nội dung vi phạm pháp luật về an ninh mạng trên dịch vụ, hệ thống thông tin do doanh nghiệp, cơ quan, tổ chức trực tiếp quản lý.

4. Về trách nhiệm của Ban Cơ yếu Chính phủ

Điều 39 Luật An ninh mạng năm 2018 quy định Ban Cơ yếu Chính phủ có trách nhiệm: (1) Tham mưu, đề xuất Bộ trưởng Bộ Quốc phòng ban hành hoặc trình cơ quan có thẩm quyền ban hành và tổ chức thực hiện văn bản quy phạm pháp luật, chương trình, kế hoạch về mật mã để bảo vệ an ninh mạng thuộc phạm vi Ban Cơ yếu Chính phủ quản lý; (2) Bảo vệ an ninh mạng đối với hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ và sản phẩm mật mã do Ban Cơ yếu Chính phủ cung cấp theo quy định của Luật An ninh mạng năm 2018; (3) Thống nhất quản lý

nghiên cứu khoa học, công nghệ mật mã; sản xuất, sử dụng, cung cấp sản phẩm mật mã để bảo vệ thông tin thuộc bí mật nhà nước được lưu trữ, trao đổi trên không gian mạng.

5. Về trách nhiệm của bộ, ngành, Ủy ban nhân dân cấp tỉnh

Điều 40 Luật An ninh mạng năm 2018 quy định trong phạm vi nhiệm vụ, quyền hạn của mình, bộ, ngành, Ủy ban nhân dân cấp tỉnh có trách nhiệm thực hiện công tác bảo vệ an ninh mạng đối với thông tin, hệ thống thông tin thuộc phạm vi quản lý; phối hợp với Bộ Công an thực hiện quản lý nhà nước về an ninh mạng của bộ, ngành, địa phương.

6. Về trách nhiệm của doanh nghiệp cung cấp dịch vụ trên không gian mạng

Điều 41 Luật An ninh mạng năm 2018 quy định doanh nghiệp cung cấp dịch vụ trên không gian mạng tại Việt Nam có trách nhiệm: (1) Cảnh báo khả năng mất an ninh mạng trong việc sử dụng dịch vụ trên không gian mạng do mình cung cấp và hướng dẫn biện pháp phòng ngừa; (2) Xây dựng phương án, giải pháp phản ứng nhanh với sự cố an ninh mạng, xử lý ngay điểm yếu, lỗ hổng bảo mật, mã độc, tấn công mạng, xâm nhập mạng và rủi ro an ninh khác; khi xảy ra sự cố an ninh mạng, ngay lập tức triển khai

phương án khẩn cấp, biện pháp ứng phó thích hợp, đồng thời báo cáo với lực lượng chuyên trách bảo vệ an ninh mạng theo quy định của Luật này; (3) Áp dụng các giải pháp kỹ thuật và các biện pháp cần thiết khác nhằm bảo đảm an ninh cho quá trình thu thập thông tin, ngăn chặn nguy cơ lộ, lọt, tổn hại hoặc mất dữ liệu; trường hợp xảy ra hoặc có nguy cơ xảy ra sự cố lộ, lọt, tổn hại hoặc mất dữ liệu thông tin người sử dụng, cần lập tức đưa ra giải pháp ứng phó, đồng thời thông báo đến người sử dụng và báo cáo với lực lượng chuyên trách bảo vệ an ninh mạng theo quy định của Luật này; (4) Phối hợp, tạo điều kiện cho lực lượng chuyên trách bảo vệ an ninh mạng trong bảo vệ an ninh mạng.

Ngoài ra, khoản 2 Điều 41 Luật An ninh mạng năm 2018 quy định doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng internet và các dịch vụ gia tăng trên không gian mạng tại Việt Nam có trách nhiệm thực hiện quy định tại khoản 2 và khoản 3 Điều 26 Luật An ninh mạng năm 2018, gồm: (1) Xác thực thông tin khi người dùng đăng ký tài khoản số; bảo mật thông tin, tài khoản của người dùng; cung cấp thông tin người dùng cho lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an khi có yêu cầu bằng văn bản để phục vụ điều tra, xử lý hành vi vi phạm pháp luật về an ninh mạng; (2) Ngăn chặn việc chia sẻ thông tin, xóa bỏ thông tin có nội dung

tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam; kích động gây bạo loạn, phá rối an ninh, gây rối trật tự công cộng; làm nhục, vu khống; xâm phạm trật tự quản lý kinh tế; bịa đặt, sai sự thật gây hoang mang trong Nhân dân, gây thiệt hại cho hoạt động kinh tế - xã hội, gây khó khăn cho hoạt động của cơ quan nhà nước hoặc người thi hành công vụ, xâm phạm quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác; trên dịch vụ hoặc hệ thống thông tin do cơ quan, tổ chức trực tiếp quản lý chậm nhất là 24 giờ kể từ thời điểm có yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an hoặc cơ quan có thẩm quyền của Bộ Thông tin và Truyền thông và lưu nhật ký hệ thống để phục vụ điều tra, xử lý hành vi vi phạm pháp luật về an ninh mạng trong thời gian theo quy định của Chính phủ; (3) Không cung cấp hoặc ngừng cung cấp dịch vụ trên mạng viễn thông, mạng internet, các dịch vụ gia tăng cho tổ chức, cá nhân đăng tải trên không gian mạng thông tin có nội dung tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam; kích động gây bạo loạn, phá rối an ninh, gây rối trật tự công cộng; làm nhục, vu khống; xâm phạm trật tự quản lý kinh tế; bịa đặt, sai sự thật gây hoang mang trong Nhân dân, gây thiệt hại cho hoạt động kinh tế - xã hội, gây khó khăn cho hoạt động của cơ quan nhà nước hoặc người thi

hành công vụ, xâm phạm quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác; khi có yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an hoặc cơ quan có thẩm quyền của Bộ Thông tin và Truyền thông; (4) Đối với doanh nghiệp trong nước và ngoài nước cung cấp dịch vụ trên mạng viễn thông, mạng internet, các dịch vụ gia tăng trên không gian mạng tại Việt Nam có hoạt động thu thập, khai thác, phân tích, xử lý dữ liệu về thông tin cá nhân, dữ liệu về mối quan hệ của người sử dụng dịch vụ, dữ liệu do người sử dụng dịch vụ tại Việt Nam tạo ra phải lưu trữ dữ liệu này tại Việt Nam trong thời gian theo quy định của Chính phủ; doanh nghiệp ngoài nước cung cấp dịch vụ trên mạng viễn thông, mạng internet, các dịch vụ gia tăng trên không gian mạng tại Việt Nam có hoạt động thu thập, khai thác, phân tích, xử lý dữ liệu về thông tin cá nhân, dữ liệu về mối quan hệ của người sử dụng dịch vụ, dữ liệu do người sử dụng dịch vụ tại Việt Nam tạo ra phải đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam.

7. Về trách nhiệm của cơ quan, tổ chức, cá nhân sử dụng không gian mạng

Điều 42 Luật An ninh mạng năm 2018 quy định cơ quan, tổ chức, cá nhân sử dụng không gian mạng có trách nhiệm: (1) Tuân thủ quy định của pháp luật về an ninh mạng; (2) Kịp thời cung

cấp thông tin liên quan đến bảo vệ an ninh mạng, nguy cơ đe dọa an ninh mạng, hành vi xâm phạm an ninh mạng cho cơ quan có thẩm quyền, lực lượng bảo vệ an ninh mạng; (3) Thực hiện yêu cầu và hướng dẫn của cơ quan có thẩm quyền trong bảo vệ an ninh mạng; giúp đỡ, tạo điều kiện cho cơ quan, tổ chức và người có trách nhiệm tiến hành các biện pháp bảo vệ an ninh mạng.

VII. VỀ ĐIỀU KHOẢN THI HÀNH

Chương VII Luật An ninh mạng năm 2018 quy định về Điều khoản thi hành (Điều 43). Theo đó, Luật An ninh mạng năm 2018 có hiệu lực thi hành từ ngày 01 tháng 01 năm 2019.

Đồng thời, Điều 43 quy định trách nhiệm của chủ quản hệ thống thông tin: (1) Bảo đảm đủ điều kiện an ninh mạng, lực lượng chuyên trách bảo vệ an ninh mạng đánh giá điều kiện an ninh mạng theo quy định tại Điều 12 của Luật này, trường hợp cần gia hạn do Thủ tướng Chính phủ quyết định nhưng không quá 12 tháng đối với hệ thống thông tin đang vận hành, sử dụng được đưa vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia, trong thời hạn 12 tháng kể từ ngày Luật có hiệu lực; (2) Bảo đảm đủ điều kiện an ninh mạng, lực lượng chuyên trách bảo vệ an ninh mạng đánh giá điều kiện an ninh mạng theo quy định tại Điều 12 của Luật này, trường hợp cần gia

hạn do Thủ tướng Chính phủ quyết định nhưng không quá 12 tháng đối với hệ thống thông tin đang vận hành, sử dụng được bổ sung vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia, trong thời hạn 12 tháng kể từ ngày được bổ sung.

Phần III

TRÁCH NHIỆM CỦA CÁC CÁ NHÂN, TỔ CHỨC TRONG BẢO VỆ AN NINH MẠNG

Luật An ninh mạng năm 2018 đã quy định rõ trách nhiệm của các cá nhân, tổ chức trong bảo vệ an ninh mạng, trong đó mọi cơ quan, tổ chức, cá nhân phải có trách nhiệm tham gia xây dựng không gian mạng lành mạnh, không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, phối hợp với các cơ quan chức năng có thẩm quyền trong áp dụng các biện pháp để bảo vệ không gian mạng quốc gia; phòng ngừa, xử lý hành vi xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân trên không gian mạng. Có thể khái quát một số nội dung cơ bản của Luật An ninh mạng năm 2018 về trách nhiệm của cá nhân, tổ chức trong bảo vệ an ninh mạng như sau:

1. Trách nhiệm bảo vệ an ninh mạng cho hệ thống thông tin quan trọng về an ninh quốc gia

Hệ thống thông tin quan trọng về an ninh quốc gia là hệ thống thông tin khi bị sự cố, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt, tấn công hoặc phá hoại sẽ xâm phạm nghiêm trọng an ninh mạng.

Chủ quản hệ thống thông tin có trách nhiệm rà soát, lập hồ sơ đề nghị đưa hệ thống thông tin thuộc thẩm quyền quản lý để đưa vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia.

Bộ Thông tin và Truyền thông có trách nhiệm gửi hồ sơ hệ thống thông tin quan trọng quốc gia đã được Thủ tướng Chính phủ phê duyệt và hồ sơ đề nghị xác định hệ thống thông tin quan trọng quốc gia cho Bộ Công an; gửi cho Bộ Công an thẩm định hồ sơ đề nghị đưa hệ thống thông tin vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia.

2. Trách nhiệm thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia

Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia, trừ hệ thống thông tin quân sự, hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ.

Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng thẩm định an ninh mạng đối với hệ thống thông tin quân sự. Ban Cơ yếu Chính phủ thẩm định an ninh mạng đối với hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ.

3. Trách nhiệm đánh giá điều kiện an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia

Theo quy định tại điểm b khoản 1 Điều 5, Điều 12 Luật An ninh mạng năm 2018, lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an đánh giá, chứng nhận đủ điều kiện an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia, trừ hệ thống thông tin quân sự, hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ.

Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng đánh giá, chứng nhận đủ điều kiện an ninh mạng đối với hệ thống thông tin quân sự.

Ban Cơ yếu Chính phủ đánh giá, chứng nhận đủ điều kiện an ninh mạng đối với hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ.

4. Trách nhiệm kiểm tra an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia

Theo quy định tại điểm c khoản 1 Điều 5, Điều 13 Luật An ninh mạng năm 2018, chủ quản hệ thống thông tin quan trọng về an ninh quốc gia có trách

nhiệm kiểm tra an ninh mạng đối với hệ thống thông tin thuộc phạm vi quản lý.

Lực lượng chuyên trách bảo vệ an ninh mạng tiến hành kiểm tra an ninh mạng đối với hệ thống thông tin theo quy định. Nội dung kiểm tra an ninh mạng, bao gồm: kiểm tra việc tuân thủ các quy định của pháp luật về bảo đảm an ninh mạng, bảo vệ bí mật nhà nước trên không gian mạng; kiểm tra, đánh giá hiệu quả các phương án, biện pháp bảo đảm an ninh mạng, phương án, kế hoạch ứng phó, khắc phục sự cố an ninh mạng; kiểm tra, đánh giá phát hiện lỗ hổng, điểm yếu bảo mật, mã độc và tấn công thử nghiệm xâm nhập hệ thống; kiểm tra, đánh giá khác do chủ quản hệ thống thông tin quy định.

5. Trách nhiệm giám sát an ninh mạng

Theo quy định điểm d khoản 1 Điều 5, Điều 14 Luật An ninh mạng năm 2018, đối với hệ thống thông tin quan trọng về an ninh quốc gia, chủ quản hệ thống thông tin có trách nhiệm chủ trì, phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng có thẩm quyền thường xuyên thực hiện giám sát an ninh mạng đối với hệ thống thông tin thuộc phạm vi quản lý; xây dựng cơ chế tự cảnh báo và tiếp nhận cảnh báo về nguy cơ đe dọa an ninh mạng, sự cố an ninh mạng, điểm yếu, lỗ hổng bảo mật, mã độc, phần cứng độc hại và đề ra phương án ứng phó, khắc phục khẩn cấp.

Lực lượng chuyên trách bảo vệ an ninh mạng có trách nhiệm thực hiện giám sát an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia thuộc phạm vi quản lý; cảnh báo và phối hợp với chủ quản hệ thống thông tin trong khắc phục, xử lý các nguy cơ đe dọa an ninh mạng, sự cố an ninh mạng, điểm yếu, lỗ hổng bảo mật, mã độc, phần cứng độc hại xảy ra đối với hệ thống thông tin quan trọng về an ninh quốc gia.

Trong trường hợp giám sát an ninh mạng phục vụ phòng ngừa, phát hiện, đấu tranh với các hành vi sử dụng không gian mạng vi phạm pháp luật, Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao thuộc Bộ Công an có trách nhiệm thực hiện giám sát an ninh mạng đối với không gian mạng quốc gia, hệ thống thông tin quan trọng về an ninh quốc gia, trừ hệ thống thông tin quân sự thuộc Bộ Quốc phòng; Bộ Tư lệnh Tác chiến không gian mạng thuộc Bộ Quốc phòng có trách nhiệm thực hiện giám sát an ninh mạng đối với hệ thống thông tin quân sự thuộc Danh mục hệ thống thông tin quan trọng về an ninh quốc gia.

Chủ quản hệ thống thông tin có trách nhiệm xây dựng, triển khai hệ thống giám sát an ninh mạng, phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng thực hiện hoạt động giám sát an ninh mạng đối với hệ thống thông tin thuộc thẩm quyền quản lý; bố trí mặt bằng, điều kiện kỹ thuật,

thiết lập, kết nối hệ thống, thiết bị giám sát của lực lượng chuyên trách bảo vệ an ninh mạng vào hệ thống thông tin do mình quản lý để phục vụ giám sát an ninh mạng; cung cấp và cập nhật thông tin về hệ thống thông tin thuộc thẩm quyền quản lý, phương án kỹ thuật triển khai hệ thống giám sát cho lực lượng chuyên trách bảo vệ an ninh mạng theo định kỳ hoặc đột xuất khi có yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng có thẩm quyền; thông báo với lực lượng chuyên trách bảo vệ an ninh mạng về hoạt động giám sát của chủ quản hệ thống thông tin định kỳ 03 tháng một lần; bảo mật các thông tin liên quan trong quá trình phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng.

Doanh nghiệp viễn thông, doanh nghiệp cung cấp dịch vụ công nghệ thông tin, viễn thông, internet có trách nhiệm phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng trong giám sát an ninh mạng theo thẩm quyền nhằm bảo vệ an ninh mạng.

6. Trách nhiệm ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia

Theo quy định tại điểm đ khoản 1 Điều 5 và Điều 15 Luật An ninh mạng năm 2018, khi phát hiện sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia, lực lượng chuyên trách bảo vệ an ninh mạng thông báo

bằng văn bản và hướng dẫn biện pháp tạm thời để ngăn chặn, xử lý hoạt động tấn công mạng, khắc phục hậu quả do tấn công mạng, sự cố an ninh mạng cho chủ quản hệ thống thông tin quan trọng về an ninh quốc gia; trường hợp khẩn cấp, thông báo bằng điện thoại hoặc các hình thức khác trước khi thông báo bằng văn bản.

Chủ quản hệ thống thông tin quan trọng về an ninh quốc gia có trách nhiệm thực hiện các biện pháp theo hướng dẫn và các biện pháp phù hợp khác để ngăn chặn, xử lý, khắc phục hậu quả ngay sau khi nhận được thông báo; trường hợp vượt quá khả năng xử lý, kịp thời thông báo cho lực lượng chuyên trách bảo vệ an ninh mạng để điều phối, ứng phó khắc phục sự cố an ninh mạng; trường hợp cần ứng phó ngay để ngăn chặn hậu quả xảy ra có khả năng gây nguy hại cho an ninh quốc gia, lực lượng chuyên trách bảo vệ an ninh mạng quyết định trực tiếp điều phối, ứng phó khắc phục sự cố an ninh mạng.

7. Trong điều phối hoạt động ứng phó, khắc phục sự cố an ninh mạng

Đối với hệ thống thông tin quan trọng về an ninh quốc gia, lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an chủ trì điều phối hoạt động ứng phó, khắc phục sự cố an ninh mạng xảy ra đối với hệ thống thông tin quan trọng về an ninh quốc gia, trừ hệ thống thông tin quân sự, hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ;

tham gia ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia khi có yêu cầu; thông báo cho chủ quản hệ thống thông tin khi phát hiện có tấn công mạng, sự cố an ninh mạng.

Chủ quản hệ thống thông tin quan trọng về an ninh quốc gia xây dựng phương án ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin thuộc phạm vi quản lý; triển khai phương án ứng phó, khắc phục khi sự cố an ninh mạng xảy ra và kịp thời báo cáo với lực lượng chuyên trách bảo vệ an ninh mạng có thẩm quyền.

Cơ quan, tổ chức, cá nhân có trách nhiệm tham gia ứng phó, khắc phục sự cố an ninh mạng xảy ra đối với hệ thống thông tin quan trọng về an ninh quốc gia khi có yêu cầu của lực lượng chủ trì điều phối; thực hiện các biện pháp, hoạt động ứng phó, khắc phục sự cố theo sự điều phối của lực lượng chuyên trách bảo vệ an ninh mạng.

8. Trách nhiệm phòng ngừa, xử lý thông tin trên không gian mạng có nội dung tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam; kích động gây bạo loạn, phá rối an ninh, gây rối trật tự công cộng; làm nhục, vu khống; xâm phạm trật tự quản lý kinh tế

Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an quyết định áp dụng biện pháp yêu cầu xóa bỏ thông tin trái pháp luật hoặc thông

tin sai sự thật trên không gian mạng xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân; quyết định tiến hành biện pháp thu thập dữ liệu điện tử để phục vụ điều tra, xử lý các hành vi xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân trên không gian mạng; quyết định đình chỉ, tạm đình chỉ hoặc yêu cầu ngừng hoạt động của hệ thống thông tin, tạm ngừng, thu hồi tên miền; yêu cầu các doanh nghiệp cung cấp dịch vụ viễn thông, dịch vụ internet, dịch vụ cung cấp nội dung trên không gian mạng và dịch vụ viễn thông giá trị gia tăng, chủ quản hệ thống thông tin xóa bỏ thông tin trái pháp luật hoặc thông tin sai sự thật trên không gian mạng xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân; yêu cầu các cơ quan, tổ chức, cá nhân có liên quan thực hiện đình chỉ, tạm đình chỉ hoặc yêu cầu ngừng hoạt động của hệ thống thông tin.

Chủ quản hệ thống thông tin có trách nhiệm triển khai biện pháp quản lý, kỹ thuật để phòng ngừa, phát hiện, ngăn chặn, gỡ bỏ thông tin trái pháp luật hoặc thông tin sai sự thật trên không gian mạng xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân trên hệ thống thông tin thuộc phạm vi quản lý khi có yêu cầu của lực

lượng chuyên trách bảo vệ an ninh mạng; phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng và cơ quan có thẩm quyền áp dụng biện pháp quy định của pháp luật để xử lý thông tin trên không gian mạng.

Tổ chức, cá nhân soạn thảo, đăng tải, phát tán thông tin trên không gian mạng phải gỡ bỏ thông tin khi có yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng và chịu trách nhiệm theo quy định của pháp luật.

9. Trách nhiệm phòng, chống gián điệp mạng; bảo vệ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên không gian mạng

Theo quy định tại Điều 17 Luật An ninh mạng năm 2018, chủ quản hệ thống thông tin kiểm tra an ninh mạng nhằm phát hiện, loại bỏ mã độc, phần cứng độc hại, khắc phục điểm yếu, lỗ hổng bảo mật; phát hiện, ngăn chặn và xử lý các hoạt động xâm nhập bất hợp pháp hoặc nguy cơ khác đe dọa an ninh mạng; triển khai biện pháp quản lý, kỹ thuật để phòng ngừa, phát hiện, ngăn chặn hành vi gián điệp mạng, xâm phạm bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên hệ thống thông tin và kịp thời gỡ bỏ thông tin liên quan đến hành vi này; phối hợp, thực hiện yêu

cầu của lực lượng chuyên trách an ninh mạng về phòng, chống gián điệp mạng, bảo vệ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên hệ thống thông tin.

Cơ quan soạn thảo, lưu trữ thông tin, tài liệu thuộc bí mật nhà nước có trách nhiệm bảo vệ bí mật nhà nước được soạn thảo, lưu giữ trên máy tính, thiết bị khác hoặc trao đổi trên không gian mạng theo quy định của pháp luật về bảo vệ bí mật nhà nước.

Bộ Công an kiểm tra an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia nhằm phát hiện, loại bỏ mã độc, phần cứng độc hại, khắc phục điểm yếu, lỗ hổng bảo mật; phát hiện, ngăn chặn, xử lý hoạt động xâm nhập bất hợp pháp; kiểm tra an ninh mạng đối với thiết bị, sản phẩm, dịch vụ thông tin liên lạc, thiết bị kỹ thuật số, thiết bị điện tử trước khi đưa vào sử dụng trong hệ thống thông tin quan trọng về an ninh quốc gia; giám sát an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia nhằm phát hiện, xử lý hoạt động thu thập trái phép thông tin thuộc bí mật nhà nước; phát hiện, xử lý các hành vi đăng tải, lưu trữ, trao đổi trái phép thông tin, tài liệu có nội dung thuộc bí mật nhà nước trên không gian mạng; tham gia nghiên cứu, sản xuất sản phẩm lưu trữ, truyền đưa thông tin, tài liệu có nội dung thuộc bí mật nhà nước;

sản phẩm mã hóa thông tin trên không gian mạng theo chức năng, nhiệm vụ được giao; thanh tra, kiểm tra công tác bảo vệ bí mật nhà nước trên không gian mạng của cơ quan nhà nước và bảo vệ an ninh mạng của chủ quản hệ thống thông tin quan trọng về an ninh quốc gia; tổ chức đào tạo, tập huấn nâng cao nhận thức và kiến thức về bảo vệ bí mật nhà nước trên không gian mạng, phòng, chống tấn công mạng, bảo vệ an ninh mạng đối với lực lượng bảo vệ an ninh mạng quy định tại khoản 2 Điều 30 Luật An ninh mạng năm 2018.

Bộ Quốc phòng có trách nhiệm thực hiện các nội dung quy định tại các điểm a, b, c, d, đ và e khoản 4 Điều 17 Luật An ninh mạng năm 2018 đối với hệ thống thông tin quân sự. Ban Cơ yếu Chính phủ có trách nhiệm tổ chức thực hiện các quy định của pháp luật trong việc sử dụng mật mã để bảo vệ thông tin thuộc bí mật nhà nước được lưu trữ, trao đổi trên không gian mạng.

10. Trách nhiệm phòng, chống tấn công mạng

Theo quy định tại khoản 8 Điều 2, Điều 19 Luật An ninh mạng năm 2018, Bộ Công an chủ trì, phối hợp với bộ, ngành có liên quan thực hiện công tác phòng ngừa, phát hiện, xử lý hành vi tấn công mạng xâm phạm hoặc đe dọa xâm phạm chủ quyền, lợi ích, an ninh quốc gia, gây tổn hại

nghiêm trọng trật tự, an toàn xã hội trên phạm vi cả nước, trừ trường hợp thuộc thẩm quyền của Bộ Quốc phòng, Ban Cơ yếu Chính phủ.

Bộ Quốc phòng chủ trì, phối hợp với bộ, ngành có liên quan thực hiện công tác phòng ngừa, phát hiện, xử lý hành vi tấn công mạng đối với hệ thống thông tin quân sự.

Ban Cơ yếu Chính phủ chủ trì, phối hợp với bộ, ngành có liên quan thực hiện công tác phòng ngừa, phát hiện, xử lý hành vi tấn công mạng đối với hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ.

Chủ quản hệ thống thông tin có trách nhiệm áp dụng biện pháp kỹ thuật để phòng ngừa, ngăn chặn hành vi tấn công mạng đối với hệ thống thông tin thuộc phạm vi quản lý.

Khi xảy ra tấn công mạng xâm phạm hoặc đe dọa xâm phạm chủ quyền, lợi ích, an ninh quốc gia, gây tổn hại nghiêm trọng trật tự, an toàn xã hội, lực lượng chuyên trách bảo vệ an ninh mạng chủ trì, phối hợp với chủ quản hệ thống thông tin và tổ chức, cá nhân có liên quan áp dụng biện pháp xác định nguồn gốc tấn công mạng, thu thập chứng cứ; yêu cầu doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng internet, các dịch vụ gia tăng trên không gian mạng chặn lọc thông tin để ngăn chặn, loại trừ hành vi tấn công mạng và cung cấp đầy đủ, kịp thời thông tin, tài liệu liên quan.

11. Trách nhiệm phòng, chống khủng bố mạng

Theo quy định tại khoản 9 Điều 2, Điều 20 Luật An ninh mạng năm 2018, chủ quản hệ thống thông tin phải thường xuyên rà soát, kiểm tra hệ thống thông tin thuộc phạm vi quản lý nhằm loại trừ nguy cơ khủng bố mạng. Khi phát hiện dấu hiệu, hành vi khủng bố mạng, cơ quan, tổ chức, cá nhân phải kịp thời báo cho lực lượng bảo vệ an ninh mạng. Cơ quan tiếp nhận tin báo có trách nhiệm tiếp nhận đầy đủ tin báo về khủng bố mạng và kịp thời thông báo cho lực lượng chuyên trách bảo vệ an ninh mạng.

Bộ Công an chủ trì, phối hợp với bộ, ngành có liên quan triển khai công tác phòng, chống khủng bố mạng, áp dụng biện pháp vô hiệu hóa nguồn khủng bố mạng, xử lý khủng bố mạng, hạn chế đến mức thấp nhất hậu quả xảy ra.

Bộ Quốc phòng chủ trì, phối hợp với bộ, ngành có liên quan triển khai công tác phòng, chống khủng bố mạng, áp dụng biện pháp xử lý khủng bố mạng xảy ra đối với hệ thống thông tin quân sự.

Ban Cơ yếu Chính phủ chủ trì, phối hợp với bộ, ngành có liên quan triển khai công tác phòng, chống khủng bố mạng, áp dụng biện pháp xử lý khủng bố mạng xảy ra đối với hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ.

12. Trách nhiệm phòng ngừa, xử lý tình huống nguy hiểm về an ninh mạng

Theo quy định tại khoản 14 Điều 2, Điều 21 Luật An ninh mạng năm 2018, lực lượng chuyên trách bảo vệ an ninh mạng phối hợp với chủ quản hệ thống thông tin quan trọng về an ninh quốc gia triển khai các giải pháp kỹ thuật, nghiệp vụ để phòng ngừa, phát hiện, xử lý tình huống nguy hiểm về an ninh mạng; quyết định áp dụng biện pháp đấu tranh bảo vệ an ninh mạng khi xảy ra các tình huống nguy hiểm về an ninh mạng; diễn ra các sự kiện chính trị quan trọng của đất nước; diễn ra các vụ tụ tập đông người, biểu tình trái pháp luật hoặc bạo loạn, phá rối an ninh, gây rối trật tự công cộng mà các biện pháp bảo vệ an ninh mạng khác đã áp dụng mà không có hiệu quả hoặc nếu không áp dụng biện pháp đấu tranh bảo vệ an ninh mạng có thể ảnh hưởng tới an ninh quốc gia; quyết định áp dụng biện pháp ngăn chặn, yêu cầu tạm ngừng, ngừng cung cấp thông tin mạng khi xảy ra một số tình huống nguy hiểm về an ninh mạng.

Doanh nghiệp viễn thông, internet, công nghệ thông tin, doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng internet, các dịch vụ gia tăng trên không gian mạng và cơ quan, tổ chức, cá nhân có liên quan có trách nhiệm phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng

thuộc Bộ Công an trong phòng ngừa, phát hiện, xử lý tình huống nguy hiểm về an ninh mạng.

Cơ quan nhà nước, tổ chức chính trị ở trung ương và địa phương phải xây dựng phương án phòng ngừa, xử lý tình huống nguy hiểm về an ninh mạng.

13. Trách nhiệm đấu tranh bảo vệ an ninh mạng

Theo quy định tại Điều 22 Luật An ninh mạng năm 2018, nội dung này được áp dụng trong trường hợp phục vụ công tác bảo vệ an ninh quốc gia theo quy định của pháp luật; xảy ra các tình huống nguy hiểm về an ninh mạng; diễn ra các sự kiện chính trị quan trọng của đất nước; diễn ra các vụ tụ tập đông người, biểu tình trái pháp luật hoặc bạo loạn, phá rối an ninh, gây rối trật tự công cộng mà các biện pháp bảo vệ an ninh mạng khác đã áp dụng mà không có hiệu quả hoặc nếu không áp dụng biện pháp đấu tranh bảo vệ an ninh mạng có thể ảnh hưởng tới an ninh quốc gia.

14. Trách nhiệm bảo vệ an ninh mạng trong cơ quan nhà nước, tổ chức chính trị ở trung ương và địa phương

Các cơ quan, tổ chức phải xây dựng, hoàn thiện quy định sử dụng mạng máy tính của cơ quan nhà nước, tổ chức chính trị ở trung ương và địa phương, xây dựng phương án bảo đảm an ninh

mạng đối với hệ thống thông tin, xây dựng phương án ứng phó, khắc phục sự cố an ninh mạng; ứng dụng, triển khai phương án, biện pháp, công nghệ bảo vệ an ninh mạng đối với hệ thống thông tin và thông tin, tài liệu được lưu trữ, soạn thảo, truyền đưa trên hệ thống thông tin thuộc phạm vi quản lý; tổ chức bồi dưỡng kiến thức về an ninh mạng cho cán bộ, công chức, viên chức, người lao động; nâng cao năng lực bảo vệ an ninh mạng cho lực lượng bảo vệ an ninh mạng; bảo vệ an ninh mạng trong hoạt động cung cấp dịch vụ công trên không gian mạng, cung cấp, trao đổi, thu thập thông tin với cơ quan, tổ chức, cá nhân, chia sẻ thông tin trong nội bộ và với cơ quan khác hoặc trong hoạt động khác theo quy định của Chính phủ; đầu tư, xây dựng hạ tầng cơ sở vật chất phù hợp với điều kiện bảo đảm triển khai hoạt động bảo vệ an ninh mạng đối với hệ thống thông tin; kiểm tra an ninh mạng đối với hệ thống thông tin; phòng, chống hành vi vi phạm pháp luật về an ninh mạng.

15. Trách nhiệm kiểm tra an ninh mạng đối với hệ thống thông tin của cơ quan, tổ chức không thuộc Danh mục hệ thống thông tin quan trọng về an ninh quốc gia

Theo quy định tại Điều 24 Luật An ninh mạng năm 2018, chủ quản hệ thống thông tin có trách nhiệm thông báo cho lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an khi phát hiện

hành vi vi phạm pháp luật về an ninh mạng trên hệ thống thông tin thuộc phạm vi quản lý.

Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an tiến hành kiểm tra an ninh mạng đối với hệ thống thông tin của cơ quan, tổ chức trong các trường hợp quy định tại khoản 1 Điều 24 Luật An ninh mạng năm 2018.

16. Trách nhiệm bảo vệ an ninh mạng đối với cơ sở hạ tầng không gian mạng quốc gia, cổng kết nối mạng quốc tế

Theo quy định tại Điều 25 Luật An ninh mạng năm 2018, trách nhiệm bảo vệ an ninh mạng đối với cơ sở hạ tầng không gian mạng quốc gia, cổng kết nối mạng quốc tế phải bảo đảm kết hợp chặt chẽ giữa yêu cầu bảo vệ an ninh mạng với yêu cầu phát triển kinh tế - xã hội; khuyến khích cổng kết nối quốc tế đặt trên lãnh thổ Việt Nam; khuyến khích tổ chức, cá nhân tham gia đầu tư xây dựng cơ sở hạ tầng không gian mạng quốc gia.

Cơ quan, tổ chức, cá nhân quản lý, khai thác cơ sở hạ tầng không gian mạng quốc gia, cổng kết nối mạng quốc tế có trách nhiệm bảo vệ an ninh mạng thuộc quyền quản lý; chịu sự quản lý, thanh tra, kiểm tra và thực hiện các yêu cầu về bảo vệ an ninh mạng của cơ quan nhà nước có thẩm quyền; tạo điều kiện, thực hiện các biện pháp kỹ thuật, nghiệp vụ cần thiết để cơ quan nhà nước có thẩm

quyền thực hiện nhiệm vụ bảo vệ an ninh mạng khi có đề nghị.

17. Trách nhiệm bảo đảm an ninh thông tin trên không gian mạng

Theo quy định tại Điều 26 Luật An ninh mạng năm 2018, doanh nghiệp trong nước và ngoài nước khi cung cấp dịch vụ trên mạng viễn thông, mạng internet, các dịch vụ gia tăng trên không gian mạng tại Việt Nam có trách nhiệm xác thực thông tin khi người dùng đăng ký tài khoản số; bảo mật thông tin, tài khoản của người dùng; cung cấp thông tin người dùng cho lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an khi có yêu cầu bằng văn bản để phục vụ điều tra, xử lý hành vi vi phạm pháp luật về an ninh mạng; ngăn chặn việc chia sẻ thông tin, xóa bỏ thông tin có nội dung quy định tại các khoản 1, 2, 3, 4 và 5 Điều 16 Luật An ninh mạng năm 2018 trên dịch vụ hoặc hệ thống thông tin do cơ quan, tổ chức trực tiếp quản lý chậm nhất là 24 giờ kể từ thời điểm có yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an hoặc cơ quan có thẩm quyền của Bộ Thông tin và Truyền thông và lưu nhật ký hệ thống để phục vụ điều tra, xử lý hành vi vi phạm pháp luật về an ninh mạng trong thời gian theo quy định của Chính phủ; không cung cấp hoặc ngừng cung cấp dịch vụ trên mạng viễn thông, mạng internet, các dịch vụ gia tăng cho tổ chức,

cá nhân đăng tải trên không gian mạng thông tin có nội dung quy định tại các khoản 1, 2, 3, 4 và 5 Điều 16 Luật An ninh mạng năm 2018 khi có yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an hoặc cơ quan có thẩm quyền của Bộ Thông tin và Truyền thông.

Về việc lưu trữ dữ liệu, đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam, khoản 3 Điều 26 Luật An ninh mạng năm 2018 quy định doanh nghiệp trong nước và ngoài nước cung cấp dịch vụ trên mạng viễn thông, mạng internet, các dịch vụ gia tăng trên không gian mạng tại Việt Nam có hoạt động thu thập, khai thác, phân tích, xử lý dữ liệu về thông tin cá nhân, dữ liệu về mối quan hệ của người sử dụng dịch vụ, dữ liệu do người sử dụng dịch vụ tại Việt Nam tạo ra phải lưu trữ dữ liệu này tại Việt Nam trong thời gian theo quy định của Chính phủ; đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam. Như vậy, việc lưu trữ dữ liệu, đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam chỉ áp dụng trong trường hợp bảo vệ an ninh quốc gia, trật tự, an toàn xã hội, đạo đức xã hội, sức khỏe cộng đồng.

Phần IV

MỘT SỐ NỘI DUNG NHÂN DÂN, DOANH NGHIỆP QUAN TÂM TRONG LUẬT AN NINH MẠNG NĂM 2018

1. Về hành vi bị nghiêm cấm

Luật An ninh mạng năm 2018 chỉ nghiêm cấm sử dụng không gian mạng để thực hiện các hành vi vi phạm pháp luật đã được pháp luật (Bộ luật Hình sự năm 2015, sửa đổi, bổ sung năm 2017, Bộ luật Dân sự năm 2015 và các văn bản quy phạm pháp luật khác liên quan) quy định, cụ thể:

- Các hành vi chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam, bao gồm sử dụng không gian mạng tổ chức, hoạt động, cấu kết, xúi giục, mua chuộc, lừa gạt, lôi kéo, đào tạo, huấn luyện người chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam, ví dụ như thông tin kích động biểu tình trái pháp luật, kích động gây rối an ninh, trật tự...

- Các hành vi xuyên tạc lịch sử, phủ nhận thành tựu cách mạng, phá hoại khối đại đoàn kết toàn dân tộc, xúc phạm tôn giáo, phân biệt đối xử về giới, phân biệt chủng tộc.

- Các hành vi phát tán thông tin gây hại cho tổ chức, cá nhân, gồm: thông tin sai sự thật gây hoang mang trong Nhân dân, gây thiệt hại cho hoạt động kinh tế - xã hội, gây khó khăn cho hoạt động của cơ quan nhà nước hoặc người thi hành công vụ, xâm phạm quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác.

- Các hành vi xâm phạm trật tự, an toàn xã hội như sử dụng không gian mạng để hoạt động mại dâm, tệ nạn xã hội, mua bán người; đăng tải thông tin dâm ô, đồi trụy, tội ác; phá hoại thuần phong, mỹ tục của dân tộc, đạo đức xã hội, sức khỏe cộng đồng, xúi giục, lôi kéo, kích động người khác phạm tội (những hành vi này đã được quy định trong Bộ luật Hình sự năm 2015, sửa đổi, bổ sung năm 2017).

- Các hành vi tấn công mạng, gián điệp mạng, khủng bố mạng và liên quan như sản xuất, đưa vào sử dụng công cụ, phương tiện, phần mềm hoặc có hành vi cản trở, gây rối loạn hoạt động của mạng viễn thông, mạng internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, phương tiện điện tử; phát tán chương trình tin học gây hại cho hoạt động của mạng viễn thông, mạng internet, mạng máy tính,

hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, phương tiện điện tử.

- Các hành vi lợi dụng quy định này của lực lượng chuyên trách để thực hiện hành vi vi phạm pháp luật (giải quyết lo ngại về lạm quyền).

Như vậy, Luật An ninh mạng năm 2018 không có quy định cấm Facebook, Google hoặc các nhà cung cấp dịch vụ nước ngoài hoạt động tại Việt Nam; không ngăn cản quyền tự do ngôn luận, quyền bày tỏ quan điểm của công dân; không cấm công dân sử dụng các dịch vụ mạng xã hội như Facebook, Google; không cấm công dân tham gia hoạt động trên không gian mạng hoặc truy cập, sử dụng thông tin trên không gian mạng.

Việc quy định hành vi bị nghiêm cấm như trên bảo đảm được:

(1) Đảm bảo thống nhất trong hệ thống pháp luật. Điều 8 Luật An ninh mạng năm 2018 - Các hành vi bị nghiêm cấm về an ninh mạng đã cụ thể hóa các hành vi cấm, hành vi vi phạm pháp luật đã được quy định trong các luật hiện hành, như: Bộ luật Hình sự năm 2015, sửa đổi, bổ sung năm 2017 (29 điều); Luật Bình đẳng giới năm 2006 (Điều 10); Luật Tín ngưỡng, tôn giáo năm 2016 (Điều 5)...

(2) Tác dụng phòng ngừa: Điều 8 và một số điều khác trong Luật An ninh mạng năm 2018 xác định rõ những hành vi bị cấm làm ranh giới cho các hoạt động trên không gian mạng.

Người dân nhận diện hành vi trái pháp luật trên không gian mạng để không vi phạm, cũng như tham gia đấu tranh, tố giác và bài trừ các hành vi này.

(3) Góp phần xây dựng không gian mạng an toàn, lành mạnh, trở thành động lực quan trọng trong phát triển kinh tế - xã hội và bảo vệ an ninh quốc gia của đất nước. Điều này đặc biệt quan trọng trong bối cảnh Việt Nam đang thúc đẩy nền kinh tế số và sẵn sàng bước vào cuộc cách mạng công nghiệp lần thứ tư.

(4) Đóng góp vào các nỗ lực chung xây dựng không gian mạng toàn cầu an toàn, lành mạnh. Việt Nam cũng như nhiều quốc gia trên thế giới đang phải đối mặt với vấn nạn tin giả (fake news), phát ngôn thù địch (hate speech), nhiều quốc gia như Đức, Thái Lan... đang có những bước đi rất mạnh mẽ để chống tin giả, phát ngôn thù địch trên không gian mạng. Hoa Kỳ và các nước phương Tây đang đẩy mạnh cuộc chiến chống tư tưởng hồi giáo cực đoan do tổ chức nhà nước Hồi giáo tự xưng (IS) và các tổ chức khủng bố tuyên truyền.

2. Về việc kiểm soát thông tin cá nhân của công dân

Điểm a khoản 2 Điều 26 Luật An ninh mạng năm 2018 quy định:

"2. Doanh nghiệp trong nước và ngoài nước cung cấp dịch vụ trên mạng viễn thông, mạng

internet, các dịch vụ gia tăng trên không gian mạng tại Việt Nam có trách nhiệm sau đây:

a) Xác thực thông tin khi người dùng đăng ký tài khoản số; bảo mật thông tin, tài khoản của người dùng; cung cấp thông tin người dùng cho lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an khi có yêu cầu bằng văn bản để phục vụ điều tra, xử lý hành vi vi phạm pháp luật về an ninh mạng".

Như vậy, doanh nghiệp trong nước và ngoài nước khi cung cấp dịch vụ trên mạng viễn thông, mạng internet và các dịch vụ gia tăng trên không gian mạng tại Việt Nam có trách nhiệm xác thực thông tin khi người dùng đăng ký tài khoản số; bảo mật thông tin, tài khoản của người dùng và chỉ trong trường hợp phục vụ điều tra, xử lý hành vi vi phạm pháp luật về an ninh mạng, lực lượng chuyên trách bảo vệ an ninh mạng mới được quyền yêu cầu cung cấp thông tin người dùng.

Thông tin cá nhân vi phạm pháp luật là một trong những loại dữ liệu quan trọng phục vụ điều tra, xử lý hành vi vi phạm pháp luật. Lực lượng bảo vệ pháp luật chỉ được phép yêu cầu cung cấp thông tin trong trường hợp phục vụ xử lý vi phạm pháp luật. Các quy định trong Bộ luật Tố tụng hình sự năm 2015 và các văn bản có liên quan đã quy định rõ về việc quản lý, sử dụng thông tin được cung cấp để phục vụ điều tra, xử lý các hành vi vi phạm pháp luật. Trước các hoạt động vi

phạm pháp luật trên không gian mạng đang diễn ra nghiêm trọng, phức tạp, yêu cầu bảo đảm cơ sở, điều kiện để điều tra, xử lý nhanh chóng, hiệu quả của lực lượng bảo vệ pháp luật là cần thiết, cấp bách, trong đó có trách nhiệm của các doanh nghiệp cung cấp dịch vụ trong và ngoài nước.

Có thông tin cho rằng, Luật An ninh mạng năm 2018 yêu cầu doanh nghiệp phải cung cấp toàn bộ thông tin người dùng như thông tin cá nhân, thông tin riêng tư cho cơ quan chức năng là không chính xác.

3. Các thông tin trên không gian mạng bị coi là vi phạm pháp luật và bị xử lý

Điều 8 và Điều 15 Luật An ninh mạng năm 2018 đã quy định 05 nhóm thông tin trên không gian mạng bị coi là vi phạm pháp luật theo quy định của Bộ luật Hình sự năm 2015 (sửa đổi, bổ sung năm 2017), gồm:

Nhóm 1: Thông tin trên không gian mạng có nội dung tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam.

Nhóm 2: Thông tin trên không gian mạng có nội dung kích động gây bạo loạn, phá rối an ninh, gây rối trật tự công cộng.

Nhóm 3: Thông tin trên không gian mạng có nội dung làm nhục, vu khống.

Nhóm 4: Thông tin trên không gian mạng có nội dung xâm phạm trật tự quản lý kinh tế.

Nhóm 5: Thông tin trên không gian mạng có nội dung sai sự thật gây hoang mang trong Nhân dân, gây thiệt hại cho các hoạt động kinh tế - xã hội, gây khó khăn cho hoạt động của cơ quan nhà nước hoặc người thi hành công vụ, xâm phạm quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác.

4. Về quản lý hoạt động kinh doanh của doanh nghiệp cung cấp dịch vụ trên không gian mạng

Hoạt động kinh doanh của doanh nghiệp không thuộc phạm vi điều chỉnh của Luật An ninh mạng năm 2018, mà thuộc phạm vi điều chỉnh của các luật khác như Luật Doanh nghiệp năm 2014, Luật Thương mại năm 2005, sửa đổi năm 2017, 2019, Luật Cạnh tranh năm 2018...

Luật An ninh mạng năm 2018 chỉ điều chỉnh nếu các dịch vụ trên không gian mạng do các doanh nghiệp này bị sử dụng vào mục đích vi phạm pháp luật, cụ thể:

- Khoản 8 Điều 16 Luật An ninh mạng năm 2018 quy định doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng internet, các dịch vụ gia tăng trên không gian mạng và chủ quản hệ thống thông tin có trách nhiệm phối hợp với cơ quan chức năng xử lý thông tin trên không gian mạng có nội dung: tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam; kích động

gây bạo loạn, phá rối an ninh, gây rối trật tự công cộng; làm nhục, vu khống; xâm phạm trật tự quản lý kinh tế; bịa đặt, sai sự thật gây hoang mang trong Nhân dân, gây thiệt hại cho hoạt động kinh tế - xã hội, gây khó khăn cho hoạt động của cơ quan nhà nước hoặc người thi hành công vụ, xâm phạm quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác.

- Khoản 3 Điều 19 Luật An ninh mạng năm 2018 quy định khi xảy ra tấn công mạng xâm phạm hoặc đe dọa xâm phạm chủ quyền, lợi ích, an ninh quốc gia, gây tổn hại nghiêm trọng trật tự, an toàn xã hội, lực lượng chuyên trách bảo vệ an ninh mạng chủ trì, phối hợp với chủ quản hệ thống thông tin và tổ chức, cá nhân có liên quan áp dụng biện pháp xác định nguồn gốc tấn công mạng, thu thập chứng cứ; yêu cầu doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng internet và các dịch vụ gia tăng trên không gian mạng chặn lọc thông tin để ngăn chặn, loại trừ hành vi tấn công mạng và cung cấp đầy đủ, kịp thời thông tin, tài liệu liên quan. Đây là hoạt động cần thiết, thuộc về trách nhiệm của các doanh nghiệp, tổ chức, cá nhân và không liên quan tới hoạt động kinh doanh của doanh nghiệp.

- Điểm b khoản 2 Điều 21 quy định: "b) Doanh nghiệp viễn thông, internet, công nghệ thông tin, doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng internet, các dịch vụ gia tăng trên

không gian mạng và cơ quan, tổ chức, cá nhân có liên quan có trách nhiệm phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an trong phòng ngừa, phát hiện, xử lý tình huống nguy hiểm về an ninh mạng".

- Tình huống nguy hiểm về an ninh mạng là sự việc xảy ra trên không gian mạng khi có hành vi xâm phạm nghiêm trọng an ninh quốc gia, gây tổn hại đặc biệt nghiêm trọng trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân. Do đó, khi xảy ra tình huống nguy hiểm về an ninh mạng, các doanh nghiệp có trách nhiệm phối hợp xử lý.

- Điều 26 Luật An ninh mạng năm 2018 quy định doanh nghiệp trong và ngoài nước khi cung cấp dịch vụ trên mạng viễn thông, mạng internet và các dịch vụ gia tăng trên không gian mạng tại Việt Nam có trách nhiệm phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng trong bảo đảm an ninh thông tin mạng.

- Khoản 2 Điều 29 Luật An ninh mạng năm 2018 quy định trách nhiệm của các doanh nghiệp trong và ngoài nước khi cung cấp dịch vụ trên mạng viễn thông, mạng internet và các dịch vụ gia tăng trên không gian mạng trong xử lý các thông tin xâm hại tới trẻ em trên không gian mạng.

- Điều 41 Luật An ninh mạng năm 2018 quy định trách nhiệm của các doanh nghiệp cung cấp dịch vụ trên không gian mạng trong ngăn chặn

xử lý các hành vi tấn công mạng, cảnh báo khả năng mất an ninh mạng và phối hợp, tạo điều kiện cho lực lượng chuyên trách bảo vệ an ninh mạng trong hoạt động bảo vệ an ninh mạng.

Như vậy, trong các quy định liên quan tới trách nhiệm của các doanh nghiệp cung cấp dịch vụ trên không gian mạng, không có quy định nào liên quan tới hoạt động kinh doanh của doanh nghiệp, hoạt động khởi nghiệp, nhập khẩu, xuất khẩu, sản xuất thiết bị của doanh nghiệp.

5. Hoạt động thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia không liên quan tới doanh nghiệp cung cấp dịch vụ trên không gian mạng

Điều 11 Luật An ninh mạng năm 2018 đã quy định rõ, đối tượng thẩm định là các hệ thống thông tin quan trọng về an ninh quốc gia. Đây là những hệ thống thông tin của cơ quan nhà nước, vị trí, vai trò, tầm quan trọng đối với an ninh quốc gia, cần được bảo vệ bằng biện pháp tương xứng.

Chủ quản hệ thống thông tin quan trọng về an ninh quốc gia phải bảo đảm cho hệ thống của mình đáp ứng các nội dung thẩm định để làm cơ sở cho việc quyết định xây dựng hoặc nâng cấp hệ thống thông tin.

Các doanh nghiệp muốn cung cấp thiết bị, sản phẩm cho hệ thống thông tin quan trọng về an

ninh quốc gia phải đáp ứng đủ các tiêu chuẩn chất lượng theo đề nghị của chủ quản hệ thống thông tin quan trọng về an ninh quốc gia, không phải đáp ứng yêu cầu từ lực lượng chuyên trách bảo vệ an ninh mạng.

6. Về quy định "giấy phép con" đối với các doanh nghiệp cung cấp dịch vụ trên không gian mạng

Trong các quy định liên quan tới trách nhiệm của các doanh nghiệp cung cấp dịch vụ trên không gian mạng trong Luật An ninh mạng năm 2018, không có quy định nào liên quan tới hoạt động kinh doanh của doanh nghiệp, cũng không có quy định nào yêu cầu các doanh nghiệp cung cấp dịch vụ trên không gian mạng phải có giấy phép con mới được phép hoạt động.

Ngoại trừ việc phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng xử lý các hành vi vi phạm pháp luật trên không gian mạng và một số trách nhiệm được quy định cụ thể trong Điều 41 Luật An ninh mạng năm 2018 liên quan tới cảnh báo, khắc phục, xử lý các hành vi vi phạm pháp luật, các doanh nghiệp không phải chấp hành nghĩa vụ nào khác đối với hoạt động kinh doanh của mình. Không có quy định nào về an ninh mạng trong Luật An ninh mạng năm 2018 quy định về hoạt động thành lập doanh nghiệp, khởi nghiệp, đầu tư, mua bán, kinh doanh của doanh nghiệp.

7. Về quy định về lưu trữ dữ liệu trong nước

Khoản 3 Điều 26 Luật An ninh mạng năm 2018 quy định:

"3. Doanh nghiệp trong nước và ngoài nước cung cấp dịch vụ trên mạng viễn thông, mạng internet, các dịch vụ gia tăng trên không gian mạng tại Việt Nam có hoạt động thu thập, khai thác, phân tích, xử lý dữ liệu về thông tin cá nhân, dữ liệu về mối quan hệ của người sử dụng dịch vụ, dữ liệu do người sử dụng dịch vụ tại Việt Nam tạo ra phải lưu trữ dữ liệu này tại Việt Nam trong thời gian theo quy định của Chính phủ.

Doanh nghiệp ngoài nước quy định tại khoản này phải đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam".

7.1. Về doanh nghiệp thuộc diện điều chỉnh

Doanh nghiệp phải chịu điều chỉnh theo quy định trên là những doanh nghiệp trong và ngoài nước cung cấp dịch vụ trên mạng viễn thông, mạng internet và các dịch vụ gia tăng trên không gian mạng tại Việt Nam có hoạt động thu thập, khai thác, phân tích, xử lý dữ liệu người dùng Việt Nam. Quy định này không áp dụng đối với toàn bộ các doanh nghiệp mà là những doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng internet và các dịch vụ gia tăng trên không gian mạng tại

Việt Nam, nhưng phải kèm theo điều kiện có hoạt động thu thập, khai thác, phân tích, xử lý dữ liệu người dùng Việt Nam. Quy định này là phù hợp với yêu cầu bảo vệ an ninh mạng hiện nay.

7.2. Về dữ liệu phải lưu trữ ở Việt Nam

Điều 26 Luật An ninh mạng năm 2018 đã quy định cụ thể ba loại dữ liệu cần lưu trữ là:

(1) Thông tin cá nhân người sử dụng dịch vụ;

(2) Dữ liệu về mối quan hệ của người sử dụng dịch vụ;

(3) Dữ liệu do người sử dụng dịch vụ tại Việt Nam tạo ra.

Như vậy, không phải toàn bộ các dữ liệu được truyền đưa trên không gian mạng phải lưu trữ tại Việt Nam. Quy định này không làm ảnh hưởng tới lưu thông dữ liệu số, cản trở hoạt động của doanh nghiệp như một số báo chí đã đưa tin thời gian qua.

7.3. Về quy định lưu trữ dữ liệu trong nước của các quốc gia trên thế giới

Theo thống kê sơ bộ, hiện đã có 18 quốc gia trên thế giới quy định phải lưu trữ dữ liệu ở trong nước, như Hoa Kỳ, Canađa, Liên bang Nga, Pháp, Đức, Trung Quốc, Ôxtrâylia, Inđônêxia, Hy Lạp, Bungari, Đan Mạch, Phần Lan, Thụy Điển, Thổ Nhĩ Kỳ, Vênêxuêla, Côlômbia, Áchentina, Braxin. Tùy vào tình hình thực tế, các quốc gia có thể yêu

cầu lưu trữ các loại dữ liệu không giống nhau. Nhiều quốc gia trên thế giới đã áp dụng các biện pháp quyết liệt hơn như truy tố đối với hành vi phỉ báng hoàng gia (Thái Lan), yêu cầu thành lập trung tâm giải quyết tin tức xấu độc (châu Âu), đặt trung tâm lưu trữ dữ liệu (Trung Quốc áp dụng với Apple), yêu cầu đặt máy chủ nếu không sẽ dừng hoạt động Facebook (Nga). Tại châu Á, nhiều quốc gia đã áp dụng chính sách quản lý chặt chẽ dữ liệu quan trọng quốc gia, trong đó có Inđônêxia, mới đây là Philíppin (xác định cấp độ các loại dữ liệu quan trọng và có chính sách quản lý tương ứng với từng loại cấp độ quản lý)[1].

Ngày 30/3/2018, vì lý do an ninh quốc gia, Bộ Ngoại giao Hoa Kỳ công bố lấy ý kiến về chính sách siết chặt kiểm soát nhập cư của Tổng thống Donald Trump, yêu cầu người nhập cảnh phải cung cấp thông tin về tài khoản mạng xã hội trong vòng 5 năm gần nhất. Đáng chú ý, không chỉ các mạng xã hội của Hoa Kỳ như Facebook, Twitter, Youtube, Flickr, Instagram, Google+, Linkedin, Pinterest, Tumbir..., mà còn yêu cầu cung cấp thông tin về tài khoản mạng xã hội của nước ngoài

---

1. Luật An ninh mạng quy định phải lưu trữ dữ liệu ở trong nước như thế nào? Cand.com.vn/Giai-dap-phap-luat/18-quoc-gia-da-quy-dinh-phai-luu-tru-du-lieu-o-trong-nuoc-496756/.

như Sina Weibo, QQ, Douban (Trung Quốc), VK (Nga)... Có thể thấy rằng, Hoa Kỳ, Anh và nhiều quốc gia khác rất quan tâm tới dữ liệu cá nhân, quyền riêng tư trên mạng xã hội bao gồm cả hai khía cạnh là thu thập và bảo vệ. Dữ liệu người dùng được coi như tài sản quốc gia, giá trị mang lại từ những dữ liệu này là không chỉ trên lĩnh vực kinh tế, chính trị và còn là an ninh quốc gia.

Như vậy, nước ta không phải quốc gia đầu tiên quy định việc lưu trữ dữ liệu và cũng không phải duy nhất là quốc gia yêu cầu lưu trữ dữ liệu trong nước.

7.4. Các cam kết quốc tế mà Việt Nam tham gia liên quan về lưu trữ dữ liệu trong nước

Quy định lưu trữ dữ liệu trong nước không trái với các cam kết quốc tế. Đã có 18 quốc gia trên thế giới quy định phải lưu trữ dữ liệu ở trong nước. Nếu vi phạm các cam kết quốc tế thì các quốc gia này đã không quy định như vậy. Mặt khác, trong các văn kiện của Tổ chức Thương mại thế giới (WTO), các Hiệp định Đối tác toàn diện và tiến bộ xuyên Thái Bình Dương (CPTPP), Hiệp định chung về thuế quan và thương mại (GATT 1994), Hiệp định chung về thương mại dịch vụ (GATS), Hiệp định về các khía cạnh liên quan đến thương mại của quyền sở hữu trí tuệ (TRIPS) đều có quy định về ngoại lệ an ninh, quy định rõ: "không có bất kỳ các quy định nào trong các văn

bản đó ngăn cản bất kỳ Thành viên nào thực hiện bất kỳ hành động nào được coi là cần thiết để bảo vệ lợi ích an ninh thiết yếu của mình".

7.5. Về quy định các doanh nghiệp nước ngoài cung cấp dịch vụ trên không gian mạng phải cung cấp thông tin người dùng cho lực lượng chuyên trách bảo vệ an ninh mạng

Tất cả các quốc gia trên thế giới đều coi an ninh quốc gia là điều kiện tiên quyết hàng đầu. Do đó, các doanh nghiệp cung cấp dịch vụ trên không gian mạng đã và đang phải phối hợp với các cơ quan chức năng của các quốc gia trên thế giới trong bảo vệ an ninh quốc gia, phòng chống tội phạm.

Khoản 2 Điều 26 Luật An ninh mạng năm 2018 đã quy định rõ các trường hợp phải cung cấp thông tin cho lực lượng chuyên trách bảo vệ an ninh mạng, cụ thể:

(1) Khi lực lượng chuyên trách bảo vệ an ninh mạng có yêu cầu bằng văn bản; và

(2) Để phục vụ điều tra, xử lý hành vi vi phạm pháp luật về an ninh mạng.

Đây là hai điều kiện đồng thời, tức là khi có hành vi vi phạm pháp luật về an ninh mạng xảy ra, khi lực lượng chuyên trách bảo vệ an ninh mạng sẽ có văn bản yêu cầu các doanh nghiệp nêu trên cung cấp thông tin về hành vi vi phạm pháp luật đó. Cần đặc biệt lưu ý rằng, những thông tin

cung cấp là thông tin liên quan tới hành vi vi phạm pháp luật.

7.6. Tác động của quy định lưu trữ dữ liệu, đặt văn phòng đại diện đối với hoạt động của các doanh nghiệp (Facebook, Google...)

Theo thống kê sơ bộ, trước Việt Nam, Google đã đặt khoảng 70 văn phòng đại diện, Facebook khoảng 80 văn phòng đại diện tại các quốc gia trên thế giới. Riêng tại khu vực Đông Nam Á, Google, Facebook đã mở văn phòng đại diện và máy chủ lưu trữ dữ liệu tại Xingapo, Inđônêxia. Hiện, Facebook đã mở thêm văn phòng đại diện tại Malaixia[1].

Quy định lưu trữ dữ liệu và đặt văn phòng đại diện không cản trở hoạt động của các doanh nghiệp (Facebook, Google...), bởi các lý do sau:

(1) Google, Facebook đều đã thuê máy chủ tại nước ta. Theo thống kê sơ bộ, Google thuê khoảng 1.781 máy chủ, Facebook thuê khoảng 441 máy chủ tại 08 doanh nghiệp cung cấp dịch vụ trong nước[2].

---

1. Nguyễn Tuyền: *Buộc Facebook, Google đặt văn phòng đại diện tại Việt Nam: "Không trái với WTO",* dantri.com.vn/Kinh-doanh/buoc-facebook-google-dat-van-phong-dai-dien-tai-viet-nam-khong-trai-voi-wto-20181103201702819.htm/.

2. Anh Thư: *Các "ông lớn" công nghệ không phải đặt máy chủ tại Việt Nam,* baogiaothong.vn/cac-ong-lon-cong-nghe-khong-phai-dat-may-chu-tai-viet-nam-d250530.htm/.

(2) Việc lưu trữ dữ liệu người sử dụng dịch vụ tại Việt Nam giúp các doanh nghiệp này tiết kiệm chi phí kinh doanh, tăng mức tốc độ truy cập và nâng cao chất lượng dịch vụ; giúp các nhà mạng trong nước tiết kiệm kinh phí khi phải mua băng thông quốc tế.

(3) Về kỹ thuật, việc lưu trữ dữ liệu trong nước được tiến hành dễ dàng khi công nghệ cho phép, nhất là áp dụng công nghệ điện toán đám mây và các doanh nghiệp này đã có sẵn kinh nghiệm và thiết bị do áp dụng tương tự ở nhiều quốc gia khác.

8. Về hệ thống thông tin quan trọng về an ninh quốc gia (Điều 10)

Hệ thống thông tin quan trọng về an ninh quốc gia được quy định tại Điều 10 Luật An ninh mạng năm 2018 là: hệ thống thông tin khi bị sự cố, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt, tấn công hoặc phá hoại sẽ xâm phạm nghiêm trọng an ninh mạng.

Với tiêu chí như trên, hệ thống thông tin quan trọng về an ninh quốc gia được xác định trong các lĩnh vực quan trọng đặc biệt đối với quốc gia như quân sự, an ninh, ngoại giao, cơ yếu; trong lĩnh vực đặc thù như lưu trữ, xử lý thông tin thuộc bí mật nhà nước; phục vụ hoạt động của các công trình quan trọng liên quan tới

an ninh quốc gia, mục tiêu quan trọng về an ninh quốc gia hoặc những hệ thống thông tin quan trọng trong các lĩnh vực năng lượng, tài chính, ngân hàng, viễn thông, giao thông vận tải, tài nguyên và môi trường, hóa chất, y tế, văn hóa, báo chí. Thủ tướng Chính phủ sẽ quy định cụ thể những hệ thống thông tin nào trong các lĩnh vực nêu trên thuộc Danh mục hệ thống thông tin quan trọng về an ninh quốc gia.

Bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia được giao cho lực lượng chuyên trách bảo vệ an ninh mạng, trực tiếp là lực lượng an ninh mạng thuộc Bộ Công an, lực lượng tác chiến không gian mạng thuộc Bộ Quốc phòng. Để bảo đảm phù hợp với hệ thống pháp luật trong nước, Luật An ninh mạng năm 2018 cũng giao Chính phủ quy định cụ thể việc phối hợp giữa Bộ Công an, Bộ Quốc phòng, Bộ Thông tin và Truyền thông, Ban Cơ yếu Chính phủ, các bộ, ngành chức năng trong việc thẩm định, đánh giá, kiểm tra, giám sát, ứng phó, khắc phục sự cố đối với hệ thống thông tin quan trọng về an ninh quốc gia.

9. Trách nhiệm và quyền lợi của cá nhân theo quy định của Luật An ninh mạng năm 2018

Theo quy định của Luật An ninh mạng năm 2018, cá nhân có trách nhiệm sau đây:

(1) Không thực hiện các hành vi bị nghiêm cấm được quy định tại Điều 8 Luật An ninh mạng năm 2018.

(2) Kịp thời cung cấp thông tin liên quan đến bảo vệ an ninh mạng, nguy cơ đe dọa an ninh mạng, hành vi xâm phạm an ninh mạng cho cơ quan quản lý nhà nước có thẩm quyền, lực lượng bảo vệ an ninh mạng.

(3) Phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng trong phòng ngừa, xử lý các hành vi sử dụng không gian mạng vi phạm pháp luật.

Cá nhân có quyền lợi sau đây:

(1) Được bảo vệ khi tham gia hoạt động trên không gian mạng trước các thông tin xấu độc xâm phạm tới danh dự, uy tín, nhân phẩm, các hoạt động tấn công mạng, gián điệp mạng, khủng bố mạng hoặc các hành vi khác gây ảnh hưởng tới quyền và lợi ích hợp pháp của mình. Với phạm vi điều chỉnh của Luật An ninh mạng năm 2018, các tổ chức, cá nhân được hoạt động trên một môi trường không gian mạng quốc gia sẽ được bảo đảm an toàn, lành mạnh hơn trước, hạn chế tối đa các yếu tố, nguy cơ xâm hại tới quyền và lợi ích hợp pháp của tổ chức, cá nhân như bị đánh cắp thông tin cá nhân, lừa đảo, chiếm đoạt tài sản, bị vu khống, làm nhục, công kích bôi nhọ, hạn chế mã độc, loại bỏ dần các hành vi đánh bạc, cá độ, tuyên truyền văn hóa phẩm đồi trụy kích động bạo lực, mại dâm và các hành vi vi phạm pháp luật khác

trên không gian mạng; bảo vệ chặt chẽ dữ liệu cá nhân trên không gian mạng; trẻ em được bảo vệ trên không gian mạng...; bảo đảm môi trường kinh doanh bình đẳng giữa các doanh nghiệp trong nước và doanh nghiệp nước ngoài về sự quản lý, tương thích với các quy định pháp luật và trách nhiệm, nghĩa vụ phải thực hiện.

(2) Được tham gia, thừa hưởng các chính sách về an ninh mạng của Nhà nước như: nghiên cứu, phát triển an ninh mạng; nâng cao năng lực tự chủ về an ninh mạng; giáo dục, bồi dưỡng kiến thức an ninh mạng.

(3) Được trao công cụ để bảo vệ quyền lợi của mình:

Điều 16 Luật An ninh mạng năm 2018 quy định về phòng ngừa, xử lý thông tin vi phạm pháp luật trên không gian mạng, quy định rõ trách nhiệm của cơ quan, tổ chức, cá nhân trong phát hiện, ngăn chặn, gỡ bỏ thông tin vi phạm pháp luật, cũng như yêu cầu lực lượng chuyên trách bảo vệ an ninh mạng tiến hành các biện pháp bảo vệ an ninh mạng để loại bỏ các thông tin vi phạm pháp luật. Điều này có nghĩa là người dân đã có công cụ rõ ràng hơn để bảo vệ mình khi bị các thông tin xấu xâm phạm quyền và lợi ích hợp pháp.

Điều 17 Luật An ninh mạng năm 2018 sẽ giúp bảo vệ người dân trước các hoạt động gián điệp mạng, bảo vệ bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên không gian mạng.

Điều 18 Luật An ninh mạng năm 2018 giúp bảo vệ người dân khỏi các hoạt động tội phạm mạng, như chiếm đoạt tài sản, trộm cắp thông tin thẻ tín dụng, tài khoản ngân hàng...

Điều 19 Luật An ninh mạng năm 2018 trao công cụ để bảo vệ người dân khỏi hoạt động tấn công mạng, như phát tán mã độc, tấn công từ chối dịch vụ...

Điều 26 Luật An ninh mạng năm 2018 tạo căn cứ pháp lý vững chắc để bảo vệ người dân khỏi các thông tin xấu độc bằng cách yêu cầu các doanh nghiệp trong và ngoài nước khi cung cấp dịch vụ trên mạng viễn thông, mạng internet và các dịch vụ gia tăng trên không gian mạng tại Việt Nam có trách nhiệm loại bỏ những nguồn phát tán thông tin xấu thông qua việc không hoặc ngừng cung cấp dịch vụ cho những đối tượng này. Đồng thời, giúp bảo vệ thông tin cá nhân, bí mật cá nhân của người dân, tránh bị thu thập và lạm dụng (trường hợp dữ liệu cá nhân người dùng Facebook bị lạm dụng vào hoạt động chính trị). Với việc yêu cầu một số doanh nghiệp nước ngoài đặt chi nhánh, văn phòng đại diện tại Việt Nam sẽ giúp người dân có quyền được quản lý, sử dụng và khiếu nại về dữ liệu của mình.

(4) Trẻ em được bảo vệ đặc biệt trên không gian mạng:

Điều 29 Luật An ninh mạng năm 2018 quy định các nội dung bảo vệ trẻ em trên không gian mạng.

Trong đó yêu cầu chủ quản hệ thống thông tin, doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng internet và các dịch vụ gia tăng trên không gian mạng, cơ quan, tổ chức, cha, mẹ, giáo viên, người chăm sóc và các cá nhân khác có trách nhiệm bảo vệ trẻ em khi trẻ em tham gia không gian mạng; yêu cầu lực lượng chuyên trách bảo vệ an ninh mạng phải áp dụng các biện pháp cần thiết để bảo vệ quyền của trẻ em trên không gian mạng.

(5) Được lực lượng chuyên trách bảo vệ an ninh mạng bảo vệ khi tham gia hoạt động trên không gian mạng, khi lực lượng chuyên trách được trao quyền thực hiện các biện pháp bảo vệ an ninh mạng cần thiết (Điều 5), giúp lực lượng này hoạt động hiệu lực, hiệu quả hơn, đồng nghĩa sẽ bảo vệ an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của tổ chức, cá nhân hữu hiệu hơn.

(6) Quyền lợi của cá nhân sẽ bảo đảm khi mọi người dân đều bình đẳng trước pháp luật. Tất cả các hành vi vi phạm pháp luật trên không gian mạng sẽ bị xử lý theo quy định của pháp luật. Trách nhiệm cộng đồng về an ninh mạng sẽ được tăng cường hơn, khi các cơ quan, tổ chức, doanh nghiệp trong quản lý hệ thống thông tin và cung cấp dịch vụ trên không gian mạng được xác định trách nhiệm cụ thể, góp phần quan trọng hình thành không gian mạng an toàn, lành mạnh.

10. Trách nhiệm và quyền lợi của doanh nghiệp theo quy định của Luật An ninh mạng năm 2018

Trách nhiệm của doanh nghiệp trong bảo vệ an ninh mạng:

(1) Khoản 8 Điều 16 Luật An ninh mạng năm 2018 quy định: Doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng internet, các dịch vụ gia tăng trên không gian mạng phải phối hợp với cơ quan chức năng xử lý các thông tin có nội dung tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam; kích động gây bạo loạn, phá rối an ninh, gây rối trật tự công cộng; làm nhục, vu khống; xâm phạm trật tự quản lý kinh tế... Đây là những thông tin vi phạm pháp luật, cần phải bị xử lý.

(2) Khoản 3 Điều 19 Luật An ninh mạng năm 2018 quy định: Doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng internet và các dịch vụ gia tăng trên không gian mạng phải phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng để ngăn chặn, loại trừ hành vi tấn công mạng. Đây là hoạt động cần thiết, thuộc về trách nhiệm, không liên quan tới hoạt động kinh doanh.

(3) Điểm b khoản 2 Điều 21 Luật An ninh mạng năm 2018 quy định: Các doanh nghiệp viễn thông, internet, công nghệ thông tin, doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng internet, các dịch vụ gia tăng trên không gian mạng có trách nhiệm phối hợp với lực lượng chuyên trách bảo vệ an

ninh mạng thuộc Bộ Công an trong phòng ngừa, phát hiện, xử lý tình huống nguy hiểm về an ninh mạng.

Tình huống nguy hiểm về an ninh mạng là sự việc xảy ra trên không gian mạng khi có hành vi xâm phạm nghiêm trọng an ninh quốc gia, gây tổn hại đặc biệt nghiêm trọng trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân. Do đó, khi xảy ra tình huống nguy hiểm về an ninh mạng, các doanh nghiệp có trách nhiệm phối hợp xử lý.

(4) Điều 26 Luật An ninh mạng năm 2018 quy định doanh nghiệp trong và ngoài nước khi cung cấp dịch vụ trên mạng viễn thông, mạng internet và các dịch vụ gia tăng trên không gian mạng tại Việt Nam có trách nhiệm phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng trong bảo đảm an ninh thông tin mạng.

(5) Khoản 2 Điều 29 Luật An ninh mạng năm 2018 quy định trách nhiệm của các doanh nghiệp trong và ngoài nước khi cung cấp dịch vụ trên mạng viễn thông, mạng internet và các dịch vụ gia tăng trên không gian mạng trong xử lý các thông tin xâm hại tới trẻ em trên không gian mạng.

(6) Điều 41 Luật An ninh mạng năm 2018 quy định trách nhiệm của các doanh nghiệp cung cấp dịch vụ trên không gian mạng trong ngăn chặn xử lý các hành vi tấn công mạng, cảnh báo khả năng mất an ninh mạng và phối hợp, tạo điều kiện cho lực lượng chuyên trách bảo vệ an ninh mạng trong hoạt động bảo vệ an ninh mạng.

Như vậy, trong 6 quy định liên quan tới trách nhiệm của các doanh nghiệp cung cấp dịch vụ trên không gian mạng, không có quy định nào liên quan tới hoạt động kinh doanh của doanh nghiệp, hoạt động khởi nghiệp, nhập khẩu, xuất khẩu, sản xuất thiết bị của doanh nghiệp.

Quyền lợi của doanh nghiệp về an ninh mạng:

(1) Được bảo vệ tốt hơn trước các hành vi vi phạm pháp luật trên không gian mạng như tung tin thất thiệt về sản phẩm, dịch vụ, cạnh tranh không lành mạnh, xâm phạm sở hữu trí tuệ, bí mật kinh doanh, chiếm đoạt tài sản, tấn công từ chối dịch vụ...

(2) Bình đẳng với các doanh nghiệp nước ngoài. Hiện nay, các doanh nghiệp viễn thông, công nghệ thông tin trong nước phải chịu nhiều ràng buộc pháp lý, từ đăng ký kinh doanh, xin cấp phép dịch vụ, thanh tra, kiểm tra, thuế, kiểm duyệt nội dung... Trong khi các doanh nghiệp cung cấp dịch vụ qua biên giới vào Việt Nam không chịu bất cứ ràng buộc nào. Điều 26 Luật An ninh mạng năm 2018 yêu cầu một số doanh nghiệp nước ngoài phải đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam. Điều này tuy không triệt để nhưng sẽ góp phần tạo môi trường kinh doanh công bằng hơn.

(3) Cạnh tranh công bằng, chống độc quyền, thao túng giá. Nhiều dịch vụ trên không gian mạng hiện nay do doanh nghiệp nước ngoài chiếm lĩnh và thao túng thị trường, tạo thế độc quyền, cạnh tranh không lành mạnh. Với quy định tại Điều 26 Luật An

ninh mạng năm 2018, các doanh nghiệp nước ngoài này phải đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam và hoạt động theo pháp luật Việt Nam.

(4) Tạo nhiều cơ hội việc làm và thu nhập. Khi các doanh nghiệp nước ngoài theo Điều 26 Luật An ninh mạng năm 2018 đặt chi nhánh, văn phòng đại diện, lưu trữ dữ liệu tại Việt Nam đồng nghĩa với cơ hội việc làm có thu nhập cao cho người Việt Nam. Các doanh nghiệp kinh doanh địa ốc, văn phòng cho thuê, cung ứng nhân lực, cung cấp hạ tầng mạng, cung cấp dịch vụ lưu trữ... cũng sẽ có những cơ hội kinh doanh mới.

(5) Cơ hội phát triển cho các doanh nghiệp công nghệ thông tin, viễn thông và an ninh mạng. Luật An ninh mạng năm 2018 hướng đến xây dựng nền công nghệ an ninh mạng tự chủ, sáng tạo (Điều 28). Do đó, đây là điều kiện thuận lợi và rất rõ ràng cho các doanh nghiệp trong nước vươn lên.

(6) Doanh nghiệp nước ngoài khi hiện diện chính thức tại Việt Nam, tuân thủ pháp luật Việt Nam, thực hiện các trách nhiệm với cộng đồng tại Việt Nam là điều kiện rất tốt để hoạt động kinh doanh, mở rộng thị trường, khách hàng, xây dựng hình ảnh trách nhiệm và đáng tin.

11. Quy định về bảo vệ thông tin cá nhân theo quy định của Luật An ninh mạng năm 2018

Điều 17 Luật An ninh mạng năm 2018 quy định các nội dung, biện pháp, trách nhiệm cụ thể của các cơ quan chức năng, doanh nghiệp và tổ

chức, cá nhân có liên quan trong bảo vệ bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên không gian mạng.

Các hành vi như chiếm đoạt, mua bán, thu giữ, cố ý làm lộ, xóa, làm hư hỏng, thất lạc, thay đổi, đưa lên không gian mạng những thông tin thuộc bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư của người khác mà chưa được phép của người sử dụng hoặc trái quy định của pháp luật sẽ bị xử lý.

Việc xác định 6 nhóm hành vi xâm phạm tới bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên không gian mạng, trách nhiệm của chủ quản hệ thống thông tin, trách nhiệm của Bộ Công an giúp cơ quan chức năng có căn cứ pháp lý để thực hiện các biện pháp phòng ngừa, đấu tranh, xử lý các hành vi này, tăng cường bảo vệ thông tin cá nhân của người sử dụng.

Trước các hoạt động vi phạm pháp luật trên không gian mạng đang diễn ra nghiêm trọng, phức tạp, yêu cầu bảo đảm cơ sở, điều kiện để điều tra, xử lý nhanh chóng, hiệu quả của lực lượng bảo vệ pháp luật là cần thiết, cấp bách, trong đó có trách nhiệm của các doanh nghiệp cung cấp dịch vụ trong và ngoài nước. Thông tin của cá nhân có hoạt động vi phạm pháp luật là một trong những loại dữ liệu quan trọng để lực lượng bảo vệ pháp luật điều tra, xử lý hành vi vi phạm pháp luật.

Điểm a khoản 2 Điều 26 Luật An ninh mạng năm 2018 quy định: "Doanh nghiệp trong và ngoài nước khi cung cấp dịch vụ trên mạng viễn thông, mạng internet, các dịch vụ gia tăng trên không gian mạng tại Việt Nam có trách nhiệm cung cấp thông tin người dùng cho lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an khi có yêu cầu bằng văn bản để phục vụ điều tra, xử lý hành vi vi phạm pháp luật về an ninh mạng".

Như vậy, lực lượng chuyên trách bảo vệ an ninh mạng chỉ được phép tiếp cận thông tin cá nhân của người sử dụng có hoạt động vi phạm pháp luật, với trình tự, thủ tục nghiêm ngặt (bằng văn bản), được các cấp có thẩm quyền phê duyệt. Hiện nay, có nhiều thông tin trên không gian mạng cho rằng, Luật An ninh mạng năm 2018 yêu cầu doanh nghiệp phải cung cấp toàn bộ thông tin người dùng như thông tin cá nhân, thông tin riêng tư cho cơ quan chức năng là không chính xác.

Luật An ninh mạng năm 2018 đã quy định rõ ràng, chỉ trong trường hợp phục vụ điều tra, xử lý hành vi vi phạm pháp luật về an ninh mạng, lực lượng chuyên trách bảo vệ an ninh mạng mới được quyền yêu cầu cung cấp thông tin người dùng.

Các quy định trong Bộ luật Tố tụng hình sự năm 2015 và các văn bản có liên quan đã quy định rõ về việc quản lý, sử dụng thông tin được cung cấp để phục vụ điều tra, xử lý các hành vi vi phạm pháp luật.

12. Quy định về thẩm định an ninh mạng theo quy định của Luật An ninh mạng năm 2018 đối với hệ thống thông tin trong nước

Chủ thể của hoạt động thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia không phải là toàn bộ hệ thống thông tin nước ta.

Điều 11 Luật An ninh mạng năm 2018 đã quy định rõ, chủ thể thẩm định là các hệ thống thông tin quan trọng về an ninh quốc gia. Đây là những hệ thống thông tin của cơ quan nhà nước, vị trí, vai trò, tầm quan trọng đối với an ninh quốc gia, cần được bảo vệ bằng biện pháp tương xứng.

Chủ quản hệ thống thông tin quan trọng về an ninh quốc gia phải bảo đảm cho hệ thống của mình đáp ứng các nội dung thẩm định để làm cơ sở cho việc quyết định xây dựng hoặc nâng cấp hệ thống thông tin.

Các doanh nghiệp muốn cung cấp thiết bị, sản phẩm cho hệ thống thông tin quan trọng về an ninh quốc gia phải đáp ứng đủ các tiêu chuẩn chất lượng theo đề nghị của chủ quản hệ thống thông tin quan trọng về an ninh quốc gia, không phải đáp ứng yêu cầu từ lực lượng chuyên trách bảo vệ an ninh mạng.

13. Quy định phòng, chống tấn công mạng trong Luật An ninh mạng năm 2018

Luật An ninh mạng năm 2018 là đạo luật đầu

tiên quy định khái niệm của hoạt động "tấn công mạng". Theo đó:

"Tấn công mạng là hành vi sử dụng không gian mạng, công nghệ thông tin hoặc phương tiện điện tử để phá hoại, gây gián đoạn hoạt động của mạng viễn thông, mạng internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử".

Đồng thời, quy định các nhóm hành vi cụ thể liên quan tới tấn công mạng tại các điều 17, 18, 19, 20 và Điều 21 Luật An ninh mạng năm 2018; quy định cụ thể các nhóm giải pháp cụ thể để phòng, chống tấn công mạng, quy định trách nhiệm cụ thể của cơ quan chức năng, chủ quản hệ thống thông tin.

Như vậy:

- Hệ thống thông tin của cơ quan, tổ chức, cá nhân được bảo vệ trước hoạt động tấn công mạng theo quy định của Luật An ninh mạng năm 2018.

- Các hệ thống thông tin quan trọng về an ninh quốc gia được bảo vệ tương xứng với tầm quan trọng đối với an ninh quốc gia, trật tự, an toàn xã hội.

- Quyền và lợi ích hợp pháp của tổ chức, cá nhân được bảo vệ trước các hành vi tấn công mạng.

Luật An ninh mạng năm 2018 cũng quy định cụ thể cơ chế phối hợp trong phòng, chống tấn công mạng của các bộ, ngành chức năng, xác định trách nhiệm cụ thể của Bộ Công an, Bộ Quốc phòng, Ban Cơ yếu Chính phủ trong phòng, chống tấn công mạng.

Phần V

MỘT SỐ VẤN ĐỀ ĐẶT RA KHI TRIỂN KHAI THI HÀNH LUẬT AN NINH MẠNG NĂM 2018 TRONG CƠ QUAN, TỔ CHỨC

Thứ nhất, nâng cao nhận thức và kiến thức bảo vệ an ninh mạng khi tham gia hoạt động trên không gian mạng của cơ quan, tổ chức, cá nhân. Cần xác định rằng, "thế giới ảo" hiện nay đã trực tiếp tác động tới quyền và lợi ích của quốc gia, tổ chức, con người. Do đó, mọi hoạt động trên không gian mạng đều phải lấy sự an toàn, an ninh, ý thức bảo vệ quyền lợi của cơ quan, tổ chức, cá nhân lên trên hết.

Về phía cơ quan nhà nước, cần chú trọng nâng cao nhận thức của lãnh đạo các cấp, cán bộ, công chức, viên chức và người lao động về bảo đảm an ninh mạng, bảo vệ chủ quyền, lợi ích, an ninh quốc gia trên không gian mạng, bảo vệ cơ sở hạ tầng không gian mạng quốc gia, cổng kết nối mạng quốc tế; chủ động đề xuất, nghiên cứu, triển khai các chính sách, giải pháp bảo vệ an ninh

mạng, phòng ngừa thông tin sai sự thật, xấu độc, chống Đảng, Nhà nước trên không gian mạng.

Lực lượng bảo vệ an ninh mạng, trực tiếp là đội ngũ cán bộ công nghệ thông tin, an toàn thông tin, an ninh mạng cần nâng cao kiến thức, kỹ năng bảo vệ an ninh mạng, khả năng xử lý các sự cố an ninh mạng, chủ động đề xuất các giải pháp bảo vệ hệ thống thông tin của cơ quan mình. Theo Nghị quyết số 30-NQ/TW ngày 25/7/2018 của Bộ Chính trị về Chiến lược an ninh mạng quốc gia, người đứng đầu cơ quan nhà nước phải chịu trách nhiệm về công tác bảo vệ hệ thống thông tin của cơ quan mình.

Về phía các tổ chức, doanh nghiệp nhà nước, cần chú trọng bảo vệ hệ thống thông tin, tập trung vào các hệ thống thông tin liên quan trực tiếp tới quyền và lợi ích của tổ chức, doanh nghiệp, các hệ thống thông tin liên quan tới thông tin, dữ liệu cá nhân của người sử dụng. Ngày 07/3/2019, Chính phủ đã ban hành Nghị quyết số 17/NQ-CP về một số nhiệm vụ, giải pháp trọng tâm phát triển Chính phủ điện tử giai đoạn 2019-2020, định hướng đến 2025, trong đó giao Bộ Công an chủ trì, phối hợp với các bộ, ngành liên quan xây dựng các văn bản hướng dẫn thi hành Luật An ninh mạng, Nghị định của Chính phủ về bảo vệ dữ liệu cá nhân. Đây là văn bản pháp luật đầu tiên của nước ta về bảo vệ dữ liệu cá nhân, tập trung quy định quyền của chủ dữ liệu cá nhân và trách nhiệm của

cơ quan, tổ chức, cá nhân có liên quan trong bảo vệ dữ liệu cá nhân.

Thứ hai, công tác tuyên truyền, phổ biến quy định của pháp luật về an ninh mạng tới mọi tầng lớp nhân dân. Tỷ lệ ứng dụng công nghệ thông tin, internet của nước ta được xếp vào trong nhóm các quốc gia có tốc độ nhanh nhất thế giới. Hiện có hơn 61 triệu người sử dụng internet, chiếm hơn 2/3 dân số[1]. Tuy nhiên, ý thức, nhận thức, kỹ năng bảo vệ bản thân trên không gian mạng chưa được chú trọng.

Về thông tin cá nhân, hầu hết người tham gia sử dụng không gian mạng đều vô tư đăng tải thông tin cá nhân, thông tin về con cái, người thân trong gia đình, không đọc kỹ điều khoản sử dụng các dịch vụ. Nhiều cơ quan, tổ chức, doanh nghiệp công khai thông tin cá nhân của khách hàng, không có biện pháp bảo vệ dữ liệu cá nhân của khách hàng, dẫn tới tình trạng bị chiếm đoạt, sử dụng, mua bán thông tin cá nhân, gây ra những hậu quả không thể lường trước về tinh thần, vật chất. Thông tin cá nhân đang được các doanh nghiệp xuyên biên giới sử dụng làm nguyên liệu để quảng cáo, sinh lợi và có trao đổi với các doanh nghiệp khác. Chỉ cần tra cứu thông tin trên Google thì Facebook đã biết và hiển thị nội dung

---

1. Nguồn: https://www.dammio.com/2018/10/08/cac-so-lieu-thong-ke-internet-viet-nam-nam-2018.

quảng cáo. Đó là chưa kể khả năng thông tin cá nhân bị sử dụng vào mục đích phạm tội, mạo danh để thực hiện hành vi vi phạm pháp luật.

Khả năng ứng phó, đề kháng trước các thông tin xấu độc của công dân còn hạn chế. Trong khi đó, việc phát tán thông tin sai sự thật, xấu độc, chống Đảng, Nhà nước của các thế lực thù địch, phản động, chống đối hiện đang diễn ra mạnh mẽ trên không gian mạng. Nhiều thông tin chỉ mang tính dư luận, đồn đoán, bịa đặt nhưng lại thu hút sự chú ý của dư luận, được chia sẻ rộng rãi trên không gian mạng. Điều 16 Luật An ninh mạng năm 2018 đã quy định cụ thể những thông tin vi phạm pháp luật. Trách nhiệm của các bộ, ngành và cơ quan nhà nước có thẩm quyền là phổ biến rộng rãi những quy định của Luật An ninh mạng năm 2018 tới mọi tầng lớp nhân dân. Đồng thời, chủ động các hình thức thông tin trên không gian mạng, dùng thông tin chính thống, kịp thời để đập tan các thông tin sai sự thật, xấu độc.

Thứ ba, tăng cường công tác bảo vệ hệ thống thông tin.

Theo kết quả kiểm tra an ninh mạng của Bộ Công an, nhiều hệ thống thông tin trong nước chưa chú trọng áp dụng các biện pháp, giải pháp bảo vệ an ninh mạng. Việc thiết kế hệ thống thông tin chưa theo các tiêu chuẩn thống nhất. Do đó, khả năng bị tấn công, xâm nhập, chiếm quyền điều khiển, chiếm đoạt bí mật nhà nước

luôn ở mức cao. Luật An ninh mạng năm 2018 đã quy định cụ thể các biện pháp bảo vệ hệ thống thông tin. Chương II quy định về các hệ thống thông tin quan trọng về an ninh quốc gia. Đây được coi là hệ thống thông tin "đầu não" nên việc bảo vệ cần được triển khai ở mức độ tương xứng. Khi được đưa vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia, các hệ thống thông tin sẽ được lực lượng chuyên trách bảo vệ an ninh mạng triển khai bảo vệ bằng quy trình, biện pháp kỹ thuật nghiêm ngặt, nâng cao tính an toàn, an ninh của hệ thống. Chương IV quy định cụ thể các biện pháp triển khai an ninh mạng trong cơ quan nhà nước. Căn cứ vào điều kiện của từng cơ quan, tổ chức, doanh nghiệp nhà nước để triển khai những nội dung phù hợp với tình hình thực tế của cơ quan mình. Các cơ quan, tổ chức, doanh nghiệp nhà nước, tổ chức chính trị xã hội cần nghiên cứu kỹ lưỡng, vận dụng trong việc bảo vệ hệ thống thông tin của mình, với tinh thần chủ động phòng ngừa, khắc phục, hạn chế sớm hậu quả, sự cố có thể xảy ra.

Thứ tư, phòng ngừa, xử lý hành vi vi phạm pháp luật trên không gian mạng.

Về trách nhiệm tham gia, phối hợp của các cơ quan, doanh nghiệp trong nước: Cùng với việc ứng dụng công nghệ thông tin sâu rộng, các hành vi sử dụng không gian mạng để phạm tội cũng gia tăng, theo chiều hướng tinh vi, phức tạp, gây hậu

quả ngày một nghiêm trọng. Đặc điểm của các hành vi phạm tội này là có tính ẩn danh cao, tính không biên giới, có tính toàn cầu, không một quốc gia, tổ chức hay lực lượng nào có thể giải quyết triệt để. Do đó, công tác phối hợp xử lý hành vi phạm tội cần có sự phối hợp, tham gia của các cơ quan chức năng có thẩm quyền, các tổ chức, doanh nghiệp, cá nhân có liên quan. Trong đó, các doanh nghiệp cung cấp dịch vụ viễn thông, internet, ứng dụng công nghệ thông tin đóng vai trò quan trọng trong việc thu thập dấu vết, chứng cứ phạm tội. Luật An ninh mạng năm 2018 đã quy định cụ thể trách nhiệm trong phòng ngừa, xử lý hành vi sử dụng không gian mạng vi phạm pháp luật. Sự phối hợp của các bên có liên quan góp phần mang lại thành công của công tác phòng ngừa, đấu tranh, xử lý tội phạm.

Về trách nhiệm của các doanh nghiệp cung cấp dịch vụ xuyên biên giới vào Việt Nam. Hiện nay, một số doanh nghiệp cung cấp dịch vụ xuyên biên giới vào Việt Nam chưa chấp hành tốt quy định của pháp luật Việt Nam. Dịch vụ của một số doanh nghiệp trở thành môi trường thực hiện các hành vi phạm tội. Thông tin sai sự thật, xấu độc, chống Đảng, Nhà nước, kích động bạo lực vẫn được phát tán trên Facebook, Youtube (Google) mà các doanh nghiệp này chưa có biện pháp ngăn chặn. Một số doanh nghiệp không chấp hành yêu cầu của cơ quan chức năng trong phòng ngừa,

xử lý tội phạm. Các doanh nghiệp này kinh doanh sinh lợi tại Việt Nam nhưng không đóng thuế, gây bất bình đẳng cho doanh nghiệp trong nước, thu thập dữ liệu cá nhân làm nguyên liệu để tiếp tục kinh doanh sinh lợi nhuận. Hiện nay, Chính phủ đang triển khai nhiều biện pháp quyết liệt. Bộ Chính trị đã ban hành Nghị quyết số 35-NQ/TW ngày 22/10/2018 về tăng cường bảo vệ nền tảng tư tưởng của Đảng, đấu tranh phản bác các quan điểm sai trái, thù địch trong tình hình mới. Thủ tướng Chính phủ đã có chỉ đạo áp dụng tổng hợp các biện pháp đối với các doanh nghiệp cung cấp dịch vụ xuyên biên giới không chấp hành quy định của pháp luật Việt Nam. Bộ Thông tin và Truyền thông đã yêu cầu các doanh nghiệp trong nước không tiếp tục quảng cáo trên nền tảng của các doanh nghiệp bị công bố là vi phạm pháp luật Việt Nam. Bộ Công an đang triển khai quy định của Luật An ninh mạng năm 2018 về việc yêu cầu các doanh nghiệp cung cấp dịch vụ xuyên biên giới bị xác định là vi phạm pháp luật Việt Nam phải lưu trữ dữ liệu, đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam, góp phần bảo vệ chủ quyền, lợi ích, an ninh quốc gia Việt Nam, làm nền tảng cho việc đấu tranh chống thất thu thuế, bảo vệ dữ liệu cá nhân của công dân Việt Nam. Việc triển khai các quy định này sẽ rất khó khăn, phức tạp và cần sự phối hợp, áp dụng đồng bộ của các cơ quan, tổ chức, doanh nghiệp trong và ngoài nước.

Thứ năm, về xây dựng không gian mạng lành mạnh. Luật An ninh mạng năm 2018 đã quy định cụ thể các quy định cần thiết để các bộ, ngành, địa phương có thể áp dụng để xây dựng không gian mạng lành mạnh, gồm: (1) Không thực hiện những hành vi bị nghiêm cấm; (2) Người dân hiểu được công cụ pháp luật được quy định trong Luật An ninh mạng năm 2018 để bảo vệ quyền lợi của mình; (3) Trẻ em được bảo vệ đặc biệt trên không gian mạng; (4) Xây dựng lực lượng bảo vệ an ninh mạng, phòng ngừa, xử lý hành vi sử dụng không gian mạng vi phạm pháp luật; (5) Các tổ chức, doanh nghiệp trong và ngoài nước bình đẳng trước pháp luật về quyền lợi, nghĩa vụ và trách nhiệm; (6) Trách nhiệm cộng đồng khi phát hiện, tố giác tin báo tội phạm. Không gian mạng cũng như xã hội chúng ta đang sống. Mỗi người có trách nhiệm chung tay bảo vệ và xây dựng thì không gian mạng sẽ an toàn, lành mạnh, lợi ích được bảo vệ tối đa.

MỤC LỤC

Chịu trách nhiệm xuất bản
Q. GIÁM ĐỐC - TỔNG BIÊN TẬP
PHẠM CHÍ THÀNH

Chịu trách nhiệm nội dung
PHÓ GIÁM ĐỐC - PHÓ TỔNG BIÊN TẬP
PGS.TS. VŨ TRỌNG LÂM

Biên tập nội dung: VĂN THỊ THANH HƯƠNG
NGUYỄN THỊ PHƯƠNG ANH
Trình bày bìa: PHẠM THÚY LIỄU
Chế bản vi tính: NGUYỄN THỊ HẰNG
Sửa bản in: TẠ THU THỦY
Đọc sách mẫu: PHƯƠNG ANH

NHÀ XUẤT BẢN CHÍNH TRỊ QUỐC GIA SỰ THẬT

Số 6/86 Duy Tân, Cầu Giấy, Hà Nội
ĐT: 080.49221, Fax: 080.49222
Email: suthat@nxbctqg.vn, Website: www.nxbctqg.vn

TÌM ĐỌC SÁCH
CỦA NHÀ XUẤT BẢN CHÍNH TRỊ QUỐC GIA SỰ THẬT

* HIẾN PHÁP NƯỚC CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM

* BỘ LUẬT HÌNH SỰ (HIỆN HÀNH) (BỘ LUẬT NĂM 2015, SỬA ĐỔI, BỔ SUNG NĂM 2017)

* BỘ LUẬT TỐ TỤNG HÌNH SỰ (HIỆN HÀNH)

XÁCH KHÔNG BÁN